

Possible References

22/3,K/3 (Item 3 from file: 350)
 DIALOG(R)File 350: Derwent WPIX
 (c) 2011 Thomson Reuters. All rights reserved.

Blu-ray disk-read only memory for use with player, records copy protection-related information and copy protection -related information recording/ non-recording identification information, as wobbled pre-pit type

Patent Assignee: KIM J Y (KIMJ-I); LG ELECTRONICS INC (GLDS); SUH S W (SUHS-I)

Inventor: KIM J; KIM J Y; SEO S U; SUH S; SUH S W

| Patent Family (9 patents, 108 countries) | | | | | | | |
|--|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| WO 2004075193 | A1 | 20040902 | WO 2004KR338 | A | 20040219 | 200461 | B |
| US 20040223427 | A1 | 20041111 | US 2003447706 | P | 20030219 | 200475 | E |
| | | | US 2004780756 | A | 20040219 | | |
| KR 2004074583 | A | 20040825 | KR 200373800 | A | 20031022 | 200501 | E |
| EP 1597730 | A1 | 20051123 | EP 2004712781 | A | 20040219 | 200577 | E |
| | | | WO 2004KR338 | A | 20040219 | | |
| TW 200423050 | A | 20041101 | TW 2004104152 | A | 20040219 | 200612 | E |
| CN 1764969 | A | 20060426 | CN 200480007952 | A | 20040219 | 200654 | E |
| JP 2006518529 | W | 20060810 | WO 2004KR338 | A | 20040219 | 200654 | E |
| | | | JP 2006502712 | A | 20040219 | | |
| US 7574003 | B2 | 20090811 | US 2004780756 | A | 20040219 | 200953 | NCE |
| CN 1764969 | B | 20101124 | CN 200480007952 | A | 20040219 | 201108 | E |

Abstract:

NOVELTY - The **blu-ray** disk-read only memory (BD-ROM) has a permanent information and control data (PIC) **zone** in which copy **protection**-related information (CPI) and identification information (CPI flag) indicating recording/non-recording of the copy **protection**-related information are recorded as a wobbled pre-pit type.... **blu-ray** disk-read only memory forming apparatus; **blu-ray** disk-read only memory reproducing apparatus; and **blu-ray** disk-read only memory reproduction method...

USE - **Blu-ray** disk-read only memory (BD-ROM) for use with recorder, player... ADVANTAGE - **Protects blu-ray** disk-read only memory from illegal copy effectively, and performs easy distinction between legal and illegal **blu-ray** disk-read only memory... Disclosed herein are a **recording medium**, an apparatus for forming the **recording medium**, and an apparatus and method for reproducing the **recording medium**. CPI (Copy **Protection**-related Information), identification information (CPI... **BD-ROM** formatter includes a copy protection control chip (CPCC). Inputted to the CPCC of the **BD-ROM** formatter is a contents **authoring code** file provided by the contents provider, which contains **control data**, such as CPI and a CPI flag, and main data such as an A/V stream. The **BD-ROM** formatter separates the control data and main data from the inputted contents **authoring code** file through the CPCC and formats the separated control data and main data such that they are suitable to a **BD-ROM** standard. Thereafter, the mastering machine makes a mass-copyable **master** using the output of the **BD-ROM** formatter inputted thereto.... For legal disc making, a legal contents **authoring code** file containing control data, such as legal CPI and a legal CPI **flag**, and **main data** is applied to the **BD-ROM** formatter. For example, here a **disc** to be legally made is of a copy protected mode type, legal **contents authoring code** file containing CPI and 'CPI_Flag=1' is inputted to the **BD-ROM** formatter. Alternatively, where a **disc** to be legally made is of a copy free mode type, a legal **contents authoring code** file containing no CPI and only 'CPI_Flag=0' is inputted to the **BD-ROM** formatter. The **BD-ROM** formatter formats the legal **control data** and **main data** separated through the CPCC such that they are suitable to the **BD-ROM** standard, and the mastering machine makes a master. However, in the case where the illegal **disc**

copying is attempted, only a **data** stream, or **main data**, illegally stored in the storage medium is inputted to the **BD-ROM** formatter, or an illegal contents **authoring code** file containing the main **data** and illegal **control data** is inputted to the **BD-ROM** formatter. In this case, the **BD-ROM** formatter formats wrong **control data** containing a CPI flag fixed at 'CPI_Flag=1' and wrong CPI or no CPI, and the **main data**... ..the **optical disc**, and compulsorily stops a data playback operation upon judging that the disc has been illegally copied. Therefore, it is possible to effectively **protect** an **optical disc** from illegal copying, make an accurate and easy distinction between a legally made **optical disc** and an illegally made **optical disc**, and... ..

Claims:

1. A **recording medium**, comprising: a specific **area** in which copy **protection**-related information and identification information indicative of recording or non-recording of the copy **protection**-related information are recorded as a wobbled pre-pit type... .. The invention claimed is: 1. A computer readable **recording medium** for use in an apparatus for reproducing data stored in the computer readable **recording medium**, comprising: a specific **area** in which copy **protection**-related information and identification information indicative of recording or non-recording of the copy **protection**-related information are recorded as a wobbled pre-pit type, the copy **protection**-related information and the identification information causing the apparatus to determine whether or not the data is copied on the computer readable **recording medium** through a legal process.

28/3,K/9 (Item 9 from file: 350)
DIALOG(R)File 350: Derwent WPIX
(c) 2011 Thomson Reuters. All rights reserved.

Files protection method e.g. for optical writable disk - having storage layer which is capable of being disrupted when laser beam of sufficient intensity is focused with disk having transparent substrate layer on one side of storage layer and lacquer layer on other side

Patent Assignee: EASTMAN KODAK CO (EAST)

Inventor: BROWNSTEIN S A; CUSHMAN T R; KLINE P J; LENTZ J P

| Patent Family (1 patents, 1 countries) | | | | | | | |
|--|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| US 5706266 | A | 19980106 | US 1991810976 | A | 19911220 | 199808 | B |
| | | | US 1992999626 | A | 19921231 | | |
| | | | US 1995432445 | A | 19950501 | | |

Abstract:

The method involves physically embedding an identification signal group in a writable **optical disk**. A second identification signal group is stored in a file written on the writable **optical disk**. On initiation of interaction between an interaction system and the writable **optical disk**, a representation of the two identification **signal** groups is transferred to a **signal** processing unit of the interaction system. The two **identification signals** group representation in the **signal** processing unit and continuing interaction are **compared** between the interaction system and the writable **optical disk** only when the **comparison** between the two **identification signal** group representations is positive... ..A transferred file is decoded prior to processing by the processing unit. Where the interaction system has a third identification **signal** group associated with it, the method involves transferring a representation of the third **identification signal** group to the **signal** processing unit of the interaction system. The third and first **identification signal** group representations are **compared** in the **signal** processing unit. Continuing interaction between the interaction system and the writable **optical disk** only when the **comparison** between the first and third **identification signal** group representations is positive... disruptions provided by the laser beam are selected to provide human readable and/or machine readable patterns. To reduce the damage to portions of the **optical disk** other than the **storage** layer, the storage layer is exposed to the laser beam prior to curing, or prior to applying and curing the lacquer layer. The **optical disk** can be of the type with data written thereon during fabrication, or the disk can be of the type in which data can be impressed thereon after fabrication of the **optical disk**. The patterns on the **optical disk** can be in the form of optical bar codes. In one application of the present invention involving the type of disk on which data can be written after fabrication...

Claims:

A method of protecting files stored on an **optical** writable **disk**, said method comprising the steps of: physically embedding a **first identification signal** group in a writable **optical disk**; storing a **second identification signal** group in a file written on said writable **optical disk**; on initiation of interaction **between** an interaction system and said writable **optical disk**, transferring a representation of said first **and** said second **identification** signal group to a signal processing unit of said interaction system; **comparing** said **first** and said **second identification signal** group representation in said signal processing... .. wherein said interaction system has a third identification signal group associated therewith, said method further comprising the steps of transferring a representation of said third **identification** signal group to the signal processing unit of said interaction system and **comparing** said third and first **identification signal** group representations in said **signal** processing unit **and** continuing interaction between said **interaction system** and said writable **optical disk** only when said **comparison** between said first and third **identification signal** group representations is positive. Basic Derwent Week: 199808

17/3,K/3 (Item 3 from file: 350)
DIALOG(R)File 350: Derwent WPIX
(c) 2011 Thomson Reuters. All rights reserved.

Cryptographic system for secure key distribution and management for DVD copy protection

Patent Assignee: INTEL CORP (ITLC)

Inventor: AUCSMITH D W

Patent Family (1 patents, 1 countries)

| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
|---------------|------|----------|--------------------|------|----------|--------|------|
| US 5915018 | A | 19990622 | US 1996740976 | A | 19961105 | 199936 | B |

Abstract:

NOVELTY - A **portion** of a digital video disc (**DVD**) is encoded with digital content **encrypted** under a content **key** which is **encrypted** under a public **key** and written out of band on **another portion** of the **disc**. An information handling system (206) is accessed by the player who receives the disc. ...
USE - For secure **key** distribution and management for **DVD** copy protection....
ADVANTAGE - The received compressed and **encrypted data** is decompressed and decrypted without exposing decrypted data or the cryptographic **keys**, as a result of which the **DVD copy** protection is not compromised....
DESCRIPTION OF DRAWINGS - The figure shows the block diagram of **cryptographic** system where access to the **DVD** content is secure... A cryptographic system and method for secure distribution and management of cryptographic **keys** for use in a **DVD** copy protection scheme is disclosed. A **DVD** disc having compressed, **encrypted content** written on a **first portion** of the disc, and the content encryption **key**, itself **encrypted** with a **second key** and written **out of band** on a **second portion** of the **disc** is used to provide **content, key**, and control information **to** a **DVD** drive according to **the** present invention. The **DVD** drive is coupled **to** a decompressor and a video controller. The video controller and **DVD** drive engage in a handshaking protocol in which all of the communication between them is **encrypted**. After verifying that the video controller is registered and not known to be compromised, the **DVD** drive passes the **content key** and control information **to** the video controller, and the compressed, **encrypted content** to the decompressor. The content decompressed by the decompressor is communicated to the video controller where it... ..

Claims:

secure distribution of digital content, comprising: a) a machine readable medium, a **first portion** of which is **encoded** with digital content **encrypted** under a content **key**, and a **second portion** of which is **encoded** out of band with a content **key** encrypted under a **public key**; b) a player **operable** to receive the machine readable medium and read the contents thereof; c) an information handling system coupled to the player; and d) a video controller... Basic Derwent Week: 199936

17/3,K/4 (Item 4 from file: 350)
 DIALOG(R)File 350: Derwent WPIX
 (c) 2011 Thomson Reuters. All rights reserved.

Information recording medium e.g. CD-ROM etc. - has key information recorded in lead-in region, and used for descrambling of data stored in data recording region

Patent Assignee: MATSUSHITA DENKI SANGYO KK (MATU); MATSUSHITA ELECTRIC IND CO LTD (MATU)

Inventor: FUKUSHIMA Y; ITO M; ITOU M; MATSUZAKI N; TATEBAYASHI M; UEDA H

| Patent Family (11 patents, 19 countries) | | | | | | | |
|--|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| WO 1997014147 | A1 | 19970417 | WO 1996JP2901 | A | 19961004 | 199721 | B |
| EP 802535 | A1 | 19971022 | EP 1996932824 | A | 19961004 | 199747 | E |
| | | | WO 1996JP2901 | A | 19961004 | | |
| JP 9514906 | X | 19971222 | WO 1996JP2901 | A | 19961004 | 199810 | E |
| | | | JP 1997514906 | A | 19961004 | | |
| US 6289102 | B1 | 20010911 | WO 1996JP2901 | A | 19961004 | 200154 | E |
| | | | US 1997849785 | A | 19971001 | | |
| JP 2004319085 | A | 20041111 | JP 1997514906 | A | 19961004 | 200474 | E |
| | | | JP 2004154000 | A | 20040524 | | |
| EP 802535 | B1 | 20050615 | EP 1996932824 | A | 19961004 | 200544 | E |
| | | | WO 1996JP2901 | A | 19961004 | | |
| | | | EP 200426324 | A | 20041105 | | |
| DE 69634850 | E | 20050721 | DE 69634850 | A | 19961004 | 200548 | E |
| | | | EP 1996932824 | A | 19961004 | | |
| | | | WO 1996JP2901 | A | 19961004 | | |
| DE 69634850 | T2 | 20060518 | DE 69634850 | A | 19961004 | 200637 | E |
| | | | EP 1996932824 | A | 19961004 | | |
| | | | WO 1996JP2901 | A | 19961004 | | |
| JP 2006179172 | A | 20060706 | JP 2004154000 | A | 19961004 | 200644 | E |
| | | | JP 20062786 | A | 20060110 | | |
| JP 3792236 | B2 | 20060705 | JP 1997514906 | A | 19961004 | 200644 | E |
| | | | JP 2004154000 | A | 20040524 | | |
| JP 2006345555 | A | 20061221 | JP 20062786 | A | 19961004 | 200703 | E |
| | | | JP 2006198385 | A | 20060720 | | |

Abstract:

The information **recording medium** has a **lead- in region** and a **data recording region**. **Key** information is recorded in the **lead-in region**, and **scrambled** data are recorded in the data recording region. **Descrambling** is performed based in the key information. First **key** information may be recorded in the **lead-in region**, and **second key** information in the data recording **region**, the **second** key information being converted based on the first key information to allow **descrambling**. . . .The data **recording region** is divided into **several sectors**, each with an sector header for identification, and a main data **region**. The **second** key information is recorded in the sector header. . . .An information **recording medium** includes a **lead-in area** and a data recording **area**. Key information is recorded in the **lead-in area**. **Scrambled** data is recorded in the data recording area. The **scrambled** data is **descrambled** based on the key information. . . .

Claims:

1. An information **recording medium** comprising a **lead-in area** and a data recording **area**, wherein key information is recorded in the **lead-in area**, **scrambled** data is recorded in the data recording area, and the **scrambled** data is descrambled based on the key information... .. An information **recording disk medium** comprising a **lead-in area** and a data recording **area**, wherein the **lead-in area** is not accessible by devices **other** than a disk reproducing device, first key information is recorded in the **lead-in area**, **scrambled** data is recorded in the data recording area and, the **scrambled** data is descrambleable based on the first key information... .. An information **recording medium** comprising a **lead-in area** not accessible by devices **other** than a disk reproducing device and a data recording area, wherein key information is recorded in the **lead-in area**, **scrambled** data is recorded in the data recording area, and the **scrambled** data is descrambled based on the key information... Basic Derwent Week: 199721

File 347: JAPI O Dec 1976-2010/ Dec(Updated 110323)

(c) 2011 JPO & JAPI O

File 350: Derwent WPI X 1963-2011/ UD=201122

(c) 2011 Thomson Reuters

| Set | Items | Description |
|-----|---------|--|
| S1 | 614723 | (RECORDING? OR RECORDABLE? OR WRITABLE? OR REWRITABLE?)(1N- (MEDIA? OR MEDIUM?) OR CD OR CDS OR CDROM? OR DVD OR DVDS OR MINIDISC? OR BLU()RAY? ? OR BLURAY? ? OR (COMPACT? OR DIGITAL- ()VERSATILE? OR MINI OR OPTICAL)() (DISC? ? OR DISK? ?) |
| S2 | 9376157 | AREA? ? OR REGION? ? OR SECTION? ? OR SECTOR? ? OR BLOCK? ? OR ZONE? ? OR PORTION? ? OR TRACK? ? |
| S3 | 394715 | S2(3N)(RECORD??? OR WRIT??? OR STOR??? OR SAV??? OR ARCHIV- ???) |
| S4 | 79717 | S3(5N)(PLURAL??? OR MULTI OR MULTIPLE OR MULTIPLICITY OR M- ULTITUDE? OR MORE(1N) ONE OR MANY OR SEVERAL? OR NUMEROUS? OR V- ARIOUS? OR SET OR SETS OR SERIES? OR COLLECTION? ? OR GROUP??- ?? OR ARRAY? ? OR TWO OR SECOND??? OR DUAL) |
| S5 | 6803 | S1(15N) S4 |
| S6 | 973425 | CODE OR CODES OR KEY OR KEYS OR SIGNATURE? ? |
| S7 | 2391 | S6(2N)(AUTHOR? ? OR AUTHORING? ? OR CREATOR? ? OR STUDIO? ? OR WRITER? ? OR PRODUCER? ? OR DISTRIBUTOR? ? OR (COPYRIGHT? OR RIGHTS)() HOLDER? ? OR OWNER? ?) OR ASC |
| S8 | 208 | S7(5N)(ENCRYPT? OR ENCOD? OR ENCIPHER? OR ENCYIPHER? OR SEC- UR? OR SCRAMBL? OR CRYPTOGRAPH?) |
| S9 | 2028122 | S2(5N)(SECOND??? OR 2ND OR ONE OR OTHER OR ANOTHER? OR DI F- FER? OR SEPARAT? OR DISTINCT? OR DISCRETE? OR LEAD() IN OR STA- RT??? OR TABLE(1W CONTENT? ? OR TOC) |
| S10 | 4 | S8(15N) S9 |
| S11 | 1507400 | S2(5N)(FIRST??? OR 1ST OR MAIN OR PRIMARY? OR DATA OR CONTE- NT? OR RECORD???? OR WRIT????) |
| S12 | 86 | S7(5N)(DECRYPT? OR DECOD? OR DECIIPHER? OR DECYIPHER? OR UNS- CRAMBL? OR UNENCRYPT? OR UNENOOD? OR UNENCIIPHER? OR UNENCYPHE- R? OR (NON OR "NOT" OR T OR WITHOUT OR NO)(1W(ENCRYPT? OR EN- COD? OR ENCIPHER? OR ENCYIPHER? OR SECUR? OR SCRAMBL?)) |
| S13 | 4 | S11(15N) S12 |
| S14 | 11 | S8(15N) S12(15N)(MATCH??? OR CORRESPOND? OR CORRELAT? OR RE- LAT? OR SAME OR IDENTICAL? OR EQUAL? OR EQUIVALEN? OR COMPAR? OR ASSOCIAT?) |
| S15 | 11 | S5 AND (S10 AND S13) OR S14 |
| S16 | 6 | (S15 AND PY=1963:2003) OR (S15 AND AY=1963:2003 AND AC=US) |
| S17 | 6 | IDPAT S16 (sorted in duplicate/non-duplicate order) |
| S18 | 49260 | S1(7N) S2 |
| S19 | 13 | S18 AND S7 |
| S20 | 13 | S19 NOT S15 |
| S21 | 10 | (S20 AND PY=1963:2003) OR (S20 AND AY=1963:2003 AND AC=US) |
| S22 | 10 | IDPAT S21 (sorted in duplicate/non-duplicate order) |
| S23 | 430 | S7(10N)(MATCH??? OR CORRESPOND? OR CORRELAT? OR RELAT? OR - SAME OR IDENTICAL? OR EQUAL? OR EQUIVALEN? OR COMPAR? OR ASSO- CIAT?) |
| S24 | 0 | S23 AND (S5 OR S18) |
| S25 | 22 | S23 AND S1 |
| S26 | 22 | S25 NOT (S15 OR S19) |
| S27 | 11 | (S26 AND PY=1963:2003) OR (S26 AND AY=1963:2003 AND AC=US) |
| S28 | 11 | IDPAT S27 (sorted in duplicate/non-duplicate order) |

File 348: EUROPEAN PATENTS 1978-201113

(c) 2011 European Patent Office

File 349: PCT FULLTEXT 1979-2011/UB=20110331|UT=20110324

(c) 2011 WPO/Thomson

| Set | Items | Description |
|-----|---------|---|
| S1 | 363915 | (RECORDING? OR RECORDABLE? OR WRITABLE? OR REWRITABLE?)(1N-) (MEDIA? OR MEDIUM?) OR CD OR CDS OR CDROM? OR DVD OR DVDS OR MINIDISC? OR BLU()RAY? ? OR BLURAY? ? OR (COMPACT? OR DIGITAL- () VERSATILE? OR MINI OR OPTICAL)() (DISC? ? OR DISK? ?) |
| S2 | 2672151 | AREA? ? OR REGION? ? OR SECTION? ? OR SECTOR? ? OR BLOCK? ? OR ZONE? ? OR PORTION? ? OR TRACK? ? |
| S3 | 208343 | S2(3N) (RECORD??? OR WRIT??? OR STOR??? OR SAV??? OR ARCHIV- ???) |
| S4 | 54432 | S3(5N) (PLURAL??? OR MULTI OR MULTIPLE OR MULTIPLICITY OR M- ULTITUDE? OR MORE(1N) ONE OR MANY OR SEVERAL? OR NUMEROUS? OR V- ARIOUS? OR SET OR SETS OR SERIES? OR COLLECTION? ? OR GROUP??- ?? OR ARRAY? ? OR TWO OR SECOND??? OR DUAL) |
| S5 | 5479 | S1(15N) S4 |
| S6 | 700700 | CODE OR CODES OR KEY OR KEYS OR SIGNATURE? ? |
| S7 | 8163 | S6(2N) (AUTHOR? ? OR AUTHORING? ? OR CREATOR? ? OR STUDIO? ? OR WRITER? ? OR PRODUCER? ? OR DISTRIBUTOR? ? OR (COPYRIGHT? OR RIGHTS)() HOLDER? ? OR OWNER? ?) OR ASC |
| S8 | 538 | S7(5N) (ENCRYPT? OR ENCOD? OR ENCIPHER? OR ENCYIPHER? OR SEC- UR? OR SCRAMBL? OR CRYPTOGRAPH?) |
| S9 | 1467712 | S2(5N) (SECOND??? OR 2ND OR ONE OR OTHER OR ANOTHER? OR DI F- FER? OR SEPARAT? OR DISTINCT? OR DISCRETE? OR LEAD() IN OR STA- RT??? OR TABLE(1W) CONTENT? ? OR TOC) |
| S10 | 40 | S8(20N) S9 |
| S11 | 893939 | S2(5N) (FIRST??? OR 1ST OR MAIN OR PRIMARY? OR DATA OR CONTE- NT? OR RECORD???? OR WRIT????) |
| S12 | 196 | S7(5N) (DECRYPT? OR DECOD? OR DECIIPHER? OR DECYIPHER? OR UNS- CRAMBL? OR UNENCRYPT? OR UNENOOD? OR UNENCIIPHER? OR UNENCYPHE- R? OR (NON OR "NOT" OR T OR WITHOUT OR NO)(1W) (ENCRYPT? OR EN- COD? OR ENCIPHER? OR ENCYIPHER? OR SECUR? OR SCRAMBL?)) |
| S13 | 17 | S11(20N) S12 |
| S14 | 28 | S8(15N) S12(15N) (MATCH??? OR CORRESPOND? OR CORRELAT? OR RE- LAT? OR SAME OR IDENTICAL? OR EQUAL? OR EQUIVALEN? OR COMPAR? OR ASSOCIAT?) |
| S15 | 0 | S5(100N) ((S10(100N) S13) OR S14) |
| S16 | 37863 | S1(7N) S2 |
| S17 | 41 | S16(100N) S7 |
| S18 | 31 | (S17 AND PY=1978:2003) OR (S17 AND AY=1978:2003 AND AC=US) |
| S19 | 31 | IDPAT S18 (sorted in duplicate/non-duplicate order) |
| S20 | 1315 | S7(10N) (MATCH??? OR CORRESPOND? OR CORRELAT? OR RELAT? OR - SAME OR IDENTICAL? OR EQUAL? OR EQUIVALEN? OR COMPAR? OR ASSO- CIAT?) |
| S21 | 20 | S20(100N) (S5 OR S16) |
| S22 | 56 | S20(100N) S1 |
| S23 | 36 | S21: S22 NOT S17 |
| S24 | 19 | (S23 AND PY=1978:2003) OR (S23 AND AY=1978:2003 AND AC=US) |
| S25 | 19 | IDPAT S24 (sorted in duplicate/non-duplicate order) |

File 8: Ei Compendex(R) 1884-2011/ Apr W
(c) 2011 Elsevier Eng. Info. Inc.
File 35: Dissertation Abs Online 1861-2011/ Mar
(c) 2011 ProQuest Info&Learning
File 65: Inside Conferences 1993-2011/ Apr 05
(c) 2011 BLDSC all rts. reserv.
File 2: INSPEC 1898-2011/ Mar W
(c) 2011 The IET
File 6: NTIS 1964-2011/ Apr W
(c) 2011 NTIS, Intl Copyright All Rights Res
File 144: Pascal 1973-2011/ Mar W
(c) 2011 INIST/CNRS
File 434: Sci Search(R) Cited Ref Sci 1974-1989/ Dec
(c) 2006 The Thomson Corp
File 34: Sci Search(R) Cited Ref Sci 1990-2011/ Mar W
(c) 2011 The Thomson Corp
File 99: Wilson Appl. Sci & Tech Abs 1983-2011/ Feb
(c) 2011 The HW Wilson Co.
File 266: FEDRI P 2011/ Jan
Comp & dist by NTIS, Intl Copyright All Rights Res
File 95: TEMA-Technology & Management 1989-2010/ Oct W
(c) 2010 FIZ TECHNIK
File 56: Computer and Information Systems Abstracts 1966-2011/ Mar
(c) 2011 CSA.
File 60: ANTE: Abstracts in New Tech & Engineer 1966-2011/ Mar
(c) 2011 CSA.
File 438: Library Lit. & Info. Science 1984-2011/ Feb
(c) 2011 The HW Wilson Co

| Set | Items | Description |
|-----|----------|---|
| S1 | 1042430 | (RECORDING? OR RECORDABLE? OR WRITABLE? OR REWRITABLE?)(1N-) (MEDIA? OR MEDIUM?) OR CD OR CDS OR CDROM? OR DVD OR DVDS OR MINIDISC? OR BLU()RAY? ? OR BLURAY? ? OR (COMPACT? OR DIGITAL- () VERSATILE? OR MINI OR OPTICAL)() (DISC? ? OR DISK? ?) |
| S2 | 12641123 | AREA? ? OR REGION? ? OR SECTION? ? OR SECTOR? ? OR BLOCK? ? OR ZONE? ? OR PORTION? ? OR TRACK? ? |
| S3 | 130415 | S2(3N) (RECORD??? OR WRIT??? OR STOR??? OR SAV??? OR ARCHIV- ???) |
| S4 | 14062 | S3(5N) (PLURAL??? OR MULTI OR MULTIPLE OR MULTIPLICITY OR M- ULTITUDE? OR MORE(1N) ONE OR MANY OR SEVERAL? OR NUMEROUS? OR V- ARIOUS? OR SET OR SETS OR SERIES? OR COLLECTION? ? OR GROUP??- ?? OR ARRAY? ? OR TWO OR SECOND??? OR DUAL) |
| S5 | 738 | S1(15N) S4 |
| S6 | 3012583 | CODE OR CODES OR KEY OR KEYS OR SIGNATURE? ? |
| S7 | 30260 | S6(2N) (AUTHOR? ? OR AUTHORING? ? OR CREATOR? ? OR STUDIO? ? OR WRITER? ? OR PRODUCER? ? OR DISTRIBUTOR? ? OR (COPYRIGHT? OR RIGHTS)() HOLDER? ? OR OWNER? ?) OR ASC |
| S8 | 566 | S7(5N) (ENCRYPT? OR ENCOD? OR ENCIPIER? OR ENCIPIER? OR SEC- UR? OR SCRAMBL? OR CRYPTOGRAPH?) |
| S9 | 1437311 | S2(5N) (SECOND??? OR 2ND OR ONE OR OTHER OR ANOTHER? OR DI F- FER? OR SEPARAT? OR DISTINCT? OR DISCRETE? OR LEAD() IN OR STA- RT??? OR TABLE(1W) CONTENT? ? OR TOC) |
| S10 | 1 | S8(20N) S9 |
| S11 | 845295 | S2(5N) (FIRST??? OR 1ST OR MAIN OR PRIMARY? OR DATA OR CONTE- NT? OR RECORD???? OR WRIT????) |
| S12 | 99 | S7(5N) (DECRYPT? OR DECOD? OR DECIPIER? OR DECIPIER? OR UNS- CRAMBL? OR UNENCRYPT? OR UNENOOD? OR UNENCIPIER? OR UNENCYPHE- R? OR (NON OR "NOT" OR T OR WITHOUT OR NO)(1W) (ENCRYPT? OR EN- COD? OR ENCIPIER? OR ENCIPIER? OR SECUR? OR SCRAMBL?)) |
| S13 | 0 | S11(20N) S12 |
| S14 | 0 | S8(15N) S12(15N) (MATCH??? OR CORRESPOND? OR CORRELAT? OR RE- LAT? OR SAME OR IDENTICAL? OR EQUAL? OR EQUIVALEN? OR COMPAR? OR ASSOCIAT?) |
| S15 | 0 | S5 AND (S10 OR S12) |

| | | |
|-----|-------|--|
| S16 | 26179 | S1(7N) S2 |
| S17 | 7 | S16 AND S7 |
| S18 | 2647 | S7(10N) (MATCH??? OR CORRESPOND? OR CORRELAT? OR RELAT? OR - SAME OR I DENTI CAL? OR EQUAL? OR EQUI VALEN? OR COMPAR? OR ASSO- CI AT?) |
| S19 | 0 | S18 AND (S5 OR S16) |
| S20 | 32 | S18 AND S1 |
| S21 | 139 | S10 OR S12 OR S17 OR S20 |
| S22 | 77 | S21 NOT PY>2003 |
| S23 | 64 | RD S22 (uni que i tems) |
| S24 | 515 | S7 AND (COPY??? OR COPI E? ? OR REPRODUC? OR DUPLI CAT?) |
| S25 | 12 | S24 AND S1 |
| S26 | 9 | S25 NOT S21 |
| S27 | 6 | S26 NOT PY>2003 |
| S28 | 6 | RD S27 (uni que i tems) |

Patent Search Results

17/3,K/1 (Item 1 from file: 350)
DIALOG(R)File 350: Derwent WPIX
(c) 2011 Thomson Reuters. All rights reserved.

Method for providing access to information on data server of electronic business card system, involves encrypting information to be sent to data user by server, on determining that server has permission to transfer information

Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)

Inventor: RICHARDS P J; TREVATHAN M B

| Patent Family (2 patents, 1 countries) | | | | | | | |
|--|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| US 20070022302 | A1 | 20070125 | US 200282693 | A | 20020222 | 200730 | B |
| | | | US 2006358812 | A | 20060221 | | |
| | | | US 2006528228 | A | 20060926 | | |
| US 7698746 | B2 | 20100413 | US 200282693 | A | 20020222 | 201027 | E |
| | | | US 2006358812 | A | 20060221 | | |
| | | | US 2006528228 | A | 20060926 | | |

Claims:

if the step of comparing the check word and the data user public key indicates that the check word and the data user public key **match**, recording permission to transfer the information in an access list; encrypting the data owner public key, by the data user, using the data user private key, to provide an **encrypted data owner public key**; sending, from the data user to the data server, the **encrypted data owner public key** and a request to transfer the information to the data user; **decrypting the encrypted data owner public key** using the data user public key, to provide a second check word; **comparing** the second check word and the data owner public key; if the step of **comparing** the second check word and the data owner public key indicates that the second check word and the data owner public key match, checking the... .. Basic Derwent Week: 200730...

17/3,K/2 (Item 2 from file: 350)
DIALOG(R)File 350: Derwent WPIX
(c) 2011 Thomson Reuters. All rights reserved.

Secure information access provision method for electronic business card system, involves permitting transfer of information in access list, if user public key and check number matches respectively with check word and preset sequence number

Patent Assignee: RICHARDS P J (RICH-I); TREVATHAN M B (TREV-I); INT BUSINESS MACHINES CORP (IBMC)

Inventor: RICHARDS P J; TREVATHAN M B

| Patent Family (2 patents, 1 countries) | | | | | | | |
|--|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| US 20060143468 | A1 | 20060629 | US 200282693 | A | 20020222 | 200652 | B |
| | | | US 2006358812 | A | 20060221 | | |
| US 7203839 | B2 | 20070410 | US 200282693 | A | 20020222 | 200726 | E |
| | | | US 2006358812 | A | 20060221 | | |

Claims:

the data server, the encrypted combination and a command that gives the data server permission to transfer the information to the data user; decrypting the **encrypted** combination, using the data

owner public key, to provide a **decrypted** combination; parsing the decrypted combination to provide a check word and a check number; **comparing** the check word and the data user public key; **comparing** the check number and an expected sequence number; if the step of comparing the check word and the data user public key indicates that the... .. and further if the step of comparing the check number and an expected sequence number indicates that the check number and the expected sequence number **match**, recording permission to transfer the information in an access list; encrypting the data owner public key, by the data user, using the data user private key, to provide an **encrypted** data owner public key; sending, from the data user to the data server, the **encrypted** data owner public key and a request to transfer the information to the data user; **decrypting** the **encrypted** data owner public key, using the data user public key, to provide a second check word; **comparing** the second check word and the data owner public key; if the step of **comparing** the second check word and the data owner public key indicates that the second check word and the data owner public key match, checking the... Basic Derwent Week: 200652

17/3,K/3 (Item 3 from file: 350)
 DIALOG(R)File 350: Derwent WPIX
 (c) 2011 Thomson Reuters. All rights reserved.

Cryptographic system for secure key distribution and management for DVD copy protection

Patent Assignee: INTEL CORP (ITLC)

Inventor: AUCSMITH D W

| Patent Family (1 patents, 1 countries) | | | | | | | |
|--|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| US 5915018 | A | 19990622 | US 1996740976 | A | 19961105 | 199936 | B |

Abstract:

NOVELTY - A **portion** of a digital video disc (**DVD**) is encoded with digital content **encrypted** under a content **key** which is **encrypted** under a public **key** and written out of band on **another portion** of the **disc**. An information handling system (206) is accessed by the player who receives the disc. ...
 USE - For secure **key** distribution and management for **DVD** copy protection.... .. ADVANTAGE - The received compressed and **encrypted data** is decompressed and decrypted without exposing decrypted data or the cryptographic **keys**, as a result of which the **DVD copy** protection is not compromised.... .. DESCRIPTION OF DRAWINGS - The figure shows the block diagram of **cryptographic** system where access to the **DVD** content is secure... A cryptographic system and method for secure distribution and management of cryptographic **keys** for use in a **DVD** copy protection scheme is disclosed. A **DVD** disc having compressed, **encrypted content** written on a **first portion** of the disc, and the content encryption **key**, itself **encrypted** with a **second key** and written **out of band on a second portion** of the **disc** is used to provide **content**, **key**, and control information **to** a **DVD** drive according to **the** present invention. The **DVD** drive is coupled **to** a decompressor and a video controller. The video controller and **DVD** drive engage in a handshaking protocol in which all of the communication between them is **encrypted**. After verifying that the video controller is registered and not known to be compromised, the **DVD** drive passes the **content key** and control information **to** the video controller, and the compressed, **encrypted content** to the decompressor. The content decompressed by the decompressor is communicated to the video controller where it... ..

Claims:

secure distribution of digital content, comprising: a) a machine readable medium, a **first portion** of which is **encoded** with digital content **encrypted** under a content **key**, and a **second portion** of which is **encoded** out of band with a content **key** encrypted under a **public key**; b) a player **operable** to receive the machine readable medium and read the contents thereof; c) an information handling system coupled to the player; and d) a video controller... Basic Derwent Week: 199936

17/3,K/4 (Item 4 from file: 350)
 DIALOG(R)File 350: Derwent WPIX
 (c) 2011 Thomson Reuters. All rights reserved.

Information recording medium e.g. CD-ROM etc. - has key information recorded in lead-in region, and used for descrambling of data stored in data recording region

Patent Assignee: MATSUSHITA DENKI SANGYO KK (MATU); MATSUSHITA ELECTRIC IND CO LTD (MATU)

Inventor: FUKUSHIMA Y; ITO M; ITOU M; MATSUZAKI N; TATEBAYASHI M; UEDA H

Patent Family (11 patents, 19 countries)

| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
|---------------|------|----------|--------------------|------|----------|--------|------|
| WO 1997014147 | A1 | 19970417 | WO 1996JP2901 | A | 19961004 | 199721 | B |
| EP 802535 | A1 | 19971022 | EP 1996932824 | A | 19961004 | 199747 | E |
| | | | WO 1996JP2901 | A | 19961004 | | |
| JP 9514906 | X | 19971222 | WO 1996JP2901 | A | 19961004 | 199810 | E |
| | | | JP 1997514906 | A | 19961004 | | |
| US 6289102 | B1 | 20010911 | WO 1996JP2901 | A | 19961004 | 200154 | E |
| | | | US 1997849785 | A | 19971001 | | |
| JP 2004319085 | A | 20041111 | JP 1997514906 | A | 19961004 | 200474 | E |
| | | | JP 2004154000 | A | 20040524 | | |
| EP 802535 | B1 | 20050615 | EP 1996932824 | A | 19961004 | 200544 | E |
| | | | WO 1996JP2901 | A | 19961004 | | |
| | | | EP 200426324 | A | 20041105 | | |
| DE 69634850 | E | 20050721 | DE 69634850 | A | 19961004 | 200548 | E |
| | | | EP 1996932824 | A | 19961004 | | |
| | | | WO 1996JP2901 | A | 19961004 | | |
| DE 69634850 | T2 | 20060518 | DE 69634850 | A | 19961004 | 200637 | E |
| | | | EP 1996932824 | A | 19961004 | | |
| | | | WO 1996JP2901 | A | 19961004 | | |
| JP 2006179172 | A | 20060706 | JP 2004154000 | A | 19961004 | 200644 | E |
| | | | JP 20062786 | A | 20060110 | | |
| JP 3792236 | B2 | 20060705 | JP 1997514906 | A | 19961004 | 200644 | E |
| | | | JP 2004154000 | A | 20040524 | | |
| JP 2006345555 | A | 20061221 | JP 20062786 | A | 19961004 | 200703 | E |
| | | | JP 2006198385 | A | 20060720 | | |

Abstract:

The information **recording medium** has a **lead- in region** and a **data** recording **region**. **Key** information is recorded in the **lead-in region**, and **scrambled** data are recorded in the data recording region. **Descrambling** is performed based in the key information. First **key** information may be recorded in the **lead-in region**, and **second key** information in the data recording **region**, the **second** key information being converted based on the first key information to allow **descrambling**... ..The data **recording region** is divided into **several sectors**, each with an sector header for identification, and a main data **region**. The **second** key information is recorded in the sector header... An information **recording medium** includes a **lead-in area** and a data recording **area**. Key information is recorded in the **lead-in area**. **Scrambled** data is recorded in the data recording area. The **scrambled** data is **descrambled** based on the key information... ..

Claims:

1. An information **recording medium** comprising a **lead-in area** and a data recording **area**, wherein

key information is recorded in the **lead-in area**, **scrambled** data is recorded in the data recording area, and the **scrambled** data is descrambled based on the key information... .. An information **recording disk medium** comprising a **lead-in area** and a data recording **area**, wherein the **lead-in area** is not accessible by devices **other** than a disk reproducing device, first key information is recorded in the **lead-in area**, **scrambled** data is recorded in the data recording area and, the **scrambled** data is descrambleable based on the first key information... .. An information **recording medium** comprising a **lead-in area** not accessible by devices **other** than a disk reproducing device and a data recording area, wherein key information is recorded in the **lead-in area**, **scrambled** data is recorded in the data recording area, and the **scrambled** data is descrambled based on the key information... Basic Derwent Week: 199721

17/3,K/5 (Item 5 from file: 350)
 DIALOG(R)File 350: Derwent WPIX
 (c) 2011 Thomson Reuters. All rights reserved.

Stored value system employing secure encryption protocol and using RF transponders for access systems - has host computer connected to read-write device over link generating secret and public key, and stores encryption data to generate validation signatures for changing transponder data, and distributes to read-write device

Patent Assignee: HID CORP (HIDH-N); PALOMAR TECHNOLOGIES CORP (PALO-N)

Inventor: RASPOTNIK W B

| Patent Family (8 patents, 5 countries) | | | | | | | |
|--|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| EP 758777 | A2 | 19970219 | EP 1996305271 | A | 19960718 | 199713 | B |
| CA 2182464 | A | 19970211 | CA 2182464 | A | 19960731 | 199724 | E |
| EP 758777 | A3 | 19970723 | EP 1996305271 | A | 19960718 | 199743 | E |
| US 5832090 | A | 19981103 | US 1995513646 | A | 19950810 | 199851 | E |
| CA 2182464 | C | 20010807 | CA 2182464 | A | 19960731 | 200148 | E |
| EP 758777 | B1 | 20020925 | EP 1996305271 | A | 19960718 | 200271 | E |
| DE 69623893 | E | 20021031 | DE 69623893 | A | 19960718 | 200279 | E |
| | | | EP 1996305271 | A | 19960718 | | |
| ES 2183915 | T3 | 20030401 | EP 1996305271 | A | 19960718 | 200328 | E |

Claims:

transponder data from the reader/writer to the central host computer, wherein the reader/writer includes means for transforming the transponder data, for decrypting the **encrypted** validation signature using the public **key**, **comparing the decrypted validation signature** to the transformed transponder data and transmitting a value change command for the stored value in response to a **match** between the **decrypted validation signature** and the transformed transponder data. Basic Derwent Week: 199713

22/3,K/1 (Item 1 from file: 350)
 DIALOG(R)File 350: Derwent WPIX
 (c) 2011 Thomson Reuters. All rights reserved.

Disk manufacture control system e.g. for DVD, issues key information to disk manufacturing entity if authenticity of key information issue request from manufacturing entity is verified

Patent Assignee: ASANO T (ASAN-I); KITANI S (KITA-I); MURAMATSU K (MURA-I); SONY CORP (SONY) ; TAKASHIMA Y (TAKA-I); YONEMITSU J (YONE-I)

Inventor: ASANO T; KITANI S; MURAMATSU K; TAKASHIMA Y; YONEMITSU; YONEMITSU J

| Patent Family (6 patents, 36 countries) | | | | | | | |
|---|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| EP 1505596 | A2 | 20050209 | EP 2004254509 | A | 20040728 | 200518 | B |
| JP 2005050176 | A | 20050224 | JP 2003282336 | A | 20030730 | 200518 | E |
| US 20050066167 | A1 | 20050324 | US 2004902212 | A | 20040728 | 200526 | E |
| CN 1601642 | A | 20050330 | CN 200410090519 | A | 20040730 | 200547 | E |
| JP 4239741 | B2 | 20090318 | JP 2003282336 | A | 20030730 | 200921 | E |
| CN 100545932 | C | 20090930 | CN 200410090519 | A | 20040730 | 201001 | E |

Abstract:

information issue request from manufacturing entity is verified. The manufacturing entity manufactures the disk storing encrypted content obtained by encrypting the content from content rights **owner** and issued **key** information... issue entity (104). The key information issue request (152) is created based on an information recording medium manufacturing request (151) issued by a content rights **owner** (102). The **key** information issue entity (104) verifies authenticity of the key information issue request (152) and, depending on the legitimacy acknowledged as a result of such verification... .. an information recording medium manufacturing entity transmits a key information issue request created based on information recording medium manufacturing request issued by a content rights **owner** to a **key** information issue entity, verifies authenticity of the issued request and, depending on the legitimacy acknowledged as a result of such verification, issues a key information...

Claims:

said content rights owning entity to perform manufacturing processing of an information recording medium storing encrypted content; and key information issue entity providing said information **recording medium** manufacturing entity with a key information **block** capable of acquiring key information for decryption of said encrypted content in response to a key information issue request from said information recording medium manufacturing... .. information recording medium manufacturing request from said content rights owning entity, and, on condition that said authorized request data is verified, provides said key information **block** for said information **recording medium** manufacturing entity; and said information recording medium manufacturing entity comprises a configuration capable of manufacturing an information recording medium storing encrypted content made by encrypting... .. request|requirement from the said content rights possession entity, and stored encryption content, It has a key information issuing entity which provides the said information **recording-medium** manufacture entity with the key information **block** which can acquire the key information which responds to the key information issue request from the said information recording-medium manufacture entity, and is applied... .. by this verification processing that they are valid request|requirement data, the said information recording-medium manufacture entity is provided with the said key information **block**, The said information **recording-medium** manufacture entity, It has the structure which manufactures the information recording medium which stored the encryption content which encrypted the receipt content from the said... .. said content rights owning entity to perform manufacturing processing of an information recording medium storing encrypted content; and key information issue entity providing said information **recording medium** manufacturing entity with a key information **block** capable of acquiring key information for decryption of said encrypted content in response to a key information issue request from said information recording medium manufacturing... .. information recording medium manufacturing request from said content rights owning entity, and, on condition that said authorized request data is verified, provides said key information **block** for said information **recording medium** manufacturing entity; and said information recording medium manufacturing entity comprises a configuration capable of manufacturing an information recording medium storing encrypted content made by encrypting...

22/3,K/2 (Item 2 from file: 350)

DIALOG(R)File 350: Derwent WPIX

(c) 2011 Thomson Reuters. All rights reserved.

Information recording medium e.g. compact disk used with personal computer, has seed

region arranged such that stored amend studio code and recording medium manufacturer code does not overlap with seed region

Patent Assignee: SONY CORP (SONY)

Inventor: ASANO T; KITANI S; MURAMATSU K; TAKASHIMA Y; YONEMITSU J; YONEMITSU

| Patent Family (5 patents, 107 countries) | | | | | | | |
|--|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| WO 2004109684 | A1 | 20041216 | WO 2004JP6619 | A | 20040511 | 200510 | B |
| US 20060150251 | A1 | 20060706 | WO 2004JP6619 | A | 20040511 | 200645 | E |
| | | | US 2005559518 | A | 20051206 | | |
| JP 2005506736 | X | 20060720 | WO 2004JP6619 | A | 20040511 | 200648 | E |
| | | | JP 2005506736 | A | 20040511 | | |
| TW 250759 | B1 | 20060301 | TW 2004112051 | A | 20040429 | 200717 | E |
| TW 200501703 | A | 20050101 | TW 2004112051 | A | 20040429 | 200958 | E |

Abstract:

NOVELTY - The information **recording medium** has **region** storing encrypted amend **studio code** (**ASC**) and **recording medium** manufacturer code (DMC). The medium has seed **region** serving as key production information, which is arranged such that none of the codes overlaps with the seed region. ... USE - Information **recording medium** e.g. **compact disk (CD)**, **digital versatile disk (DVD)**, **DVD-ROM**, **DVD-video ROM**, hard disk and **mini disk (MD)** used with personal computer (PC), **CD** player, **DVD** player, MD player and game machine for recording content such as image data, audio data, music, movie, game program and other application program... ... ADVANTAGE - Prevents the leakage of entity codes in the information **recording medium**.... ... DESCRIPTION OF DRAWINGS - The figure shows the storage position of encrypted amend **studio code** and **recording medium** manufacturer code in the information **recording medium**. (Drawing includes non-English language text) The present invention provides a configuration for preventing each entity code stored in information **recording media** from being leaked. **Authoring studio code (ASC)** and disc manufacturer code (DMC) are encrypted without failure and the encrypted codes are stored in information **recording media**. The data setting location in program map table (PMT) is controlled such that these entity codes will not overlap the seed area that provides key generating information, so that, if the packet storing the program map table storing **authoring studio code (ASC)** and disc manufacturer code (DMC) is set to an arbitrary position in a content packet sequence, these entity codes will not overlap the seed area... ... An arrangement for preventing leakage of entity codes stored in an information **recording medium**. The arrangement ensures that amend **studio code (ASC)** and information **recording medium** manufacturer code (DMC) are encrypted and stored in an information **recording medium**. The data setting positions in a program map table (PMT) are controlled such that none of those codes overlaps with a seed region serving as key production information. As a result, even if the stored packets of the program map table storing therein the amend **studio code (ASC)** and information **recording medium** manufacturer code (DMC) are set to any position in the content packet sequence, then none of the entity codes overlaps with the seed region serving... ...

Claims:

1. An information **recording medium** storing encrypted content, having a configuration in which content and an entity code set for each entity in a manufacturing route of said information **recording medium**, and data included in a certain encryption processing unit is encrypted by a key generated on the basis of a seed providing encryption processing key...

22/3,K/3 (Item 3 from file: 350)

DIALOG(R)File 350: Derwent WPIX

(c) 2011 Thomson Reuters. All rights reserved.

Blu-ray disk-read only memory for use with player, records copy protection-related information and copy protection -related information recording/ non-recording

identification information, as wobbled pre-pit type

Patent Assignee: KIM J Y (KIMJ-I); LG ELECTRONICS INC (GLDS); SUH S W (SUHS-I)

Inventor: KIM J; KIM J Y; SEO S U; SUH S; SUH S W

| Patent Family (9 patents, 108 countries) | | | | | | | |
|--|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| WO 2004075193 | A1 | 20040902 | WO 2004KR338 | A | 20040219 | 200461 | B |
| US 20040223427 | A1 | 20041111 | US 2003447706 | P | 20030219 | 200475 | E |
| | | | US 2004780756 | A | 20040219 | | |
| KR 2004074583 | A | 20040825 | KR 200373800 | A | 20031022 | 200501 | E |
| EP 1597730 | A1 | 20051123 | EP 2004712781 | A | 20040219 | 200577 | E |
| | | | WO 2004KR338 | A | 20040219 | | |
| TW 200423050 | A | 20041101 | TW 2004104152 | A | 20040219 | 200612 | E |
| CN 1764969 | A | 20060426 | CN 200480007952 | A | 20040219 | 200654 | E |
| JP 2006518529 | W | 20060810 | WO 2004KR338 | A | 20040219 | 200654 | E |
| | | | JP 2006502712 | A | 20040219 | | |
| US 7574003 | B2 | 20090811 | US 2004780756 | A | 20040219 | 200953 | NCE |
| CN 1764969 | B | 20101124 | CN 200480007952 | A | 20040219 | 201108 | E |

Abstract:

NOVELTY - The **blu-ray** disk-read only memory (BD-ROM) has a permanent information and control data (PIC) **zone** in which copy **protection**-related information (CPI) and identification information (CPI f lag) indicating recording/non-recording of the copy **protection**-related information are recorded as a wobbled pre-pit type.... **blu-ray** disk-read only memory forming apparatus; **blu-ray** disk-read only memory reproducing apparatus; and **blu-ray** disk-read only memory reproduction method... ... USE - **Blu-ray** disk-read only memory (BD-ROM) for use with recorder, player... ... ADVANTAGE - **Protects blu-ray** disk-read only memory from illegal copy effectively, and performs easy distinction between legal and illegal **blu-ray** disk-read only memory... ... Disclosed herein are a **recording medium**, an apparatus for forming the **recording medium**, and an apparatus and method for reproducing the **recording medium**. CPI (Copy **Protection**-related Information), identification information (CPI... ... **BD-ROM** formatter includes a copy protection control chip (CPCC). Inputted to the CPCC of the **BD-ROM** formatter is a contents **authoring code** file provided by the contents provider, which contains **control data**, such as CPI and a CPI flag, and main data such as an A/V stream. The **BD-ROM** formatter separates the control data and main data from the inputted contents **authoring code** file through the CPCC and formats the separated control data and main data such that they are suitable to a **BD-ROM** standard. Thereafter, the mastering machine makes a mass-copyable **master** using the output of the **BD-ROM** formatter inputted thereto.... ... For legal disc making, a legal contents **authoring code** file containing control data, such as legal CPI and a legal CPI **flag**, and **main data** is applied to the **BD-ROM** formatter. For example, here a **disc** to be legally made is of a copy protected mode type, legal **contents authoring code** file containing CPI and 'CPI_Flag=1' is inputted to the **BD-ROM** formatter. Alternatively, where a **disc** to be legally made is of a copy free mode type, a legal **contents authoring code** file containing no CPI and only 'CPI_Flag=0' is inputted to the **BD-ROM** formatter. The **BD-ROM** formatter formats the legal **control data** and **main data** separated through the CPCC such that they are suitable to the **BD-ROM** standard, and the mastering machine makes a master. However, in the case where the illegal **disc** copying is attempted, only a **data** stream, or **main data**, illegally stored in the storage medium is inputted to the **BD-ROM** formatter, or an illegal contents **authoring code** file containing the main **data** and illegal **control data** is inputted to the **BD-ROM** formatter. In this case, the **BD-ROM** formatter formats wrong **control data** containing a CPI flag fixed at 'CPI_Flag=1' and wrong CPI or no CPI, and the **main data**.... ...the **optical disc**, and compulsorily stops a data playback operation upon judging that the disc has been illegally copied. Therefore, it is possible to effectively **protect** an **optical disc** from illegal copying, make an accurate and easy distinction between a legally made **optical disc** and an illegally made **optical disc**, and... ...

Claims:

1. A **recording medium**, comprising: a specific **area** in which copy **protection**-related information and identification information indicative of recording or non-recording of the copy **protection**-related information are recorded as a wobbled pre-pit type... .. The invention claimed is: 1. A computer readable **recording medium** for use in an apparatus for reproducing data stored in the computer readable **recording medium**, comprising: a specific **area** in which copy **protection**-related information and identification information indicative of recording or non-recording of the copy **protection**-related information are recorded as a wobbled pre-pit type, the copy **protection**-related information and the identification information causing the apparatus to determine whether or not the data is copied on the computer readable **recording medium** through a legal process.

22/3,K/4 (Item 4 from file: 350)

DIALOG(R)File 350: Derwent WPIX

(c) 2011 Thomson Reuters. All rights reserved.

Authoring apparatus for video CD, has data output portion to group the keys with which contents have been encrypted, encrypt grouped keys, create grouped encrypted keys and output contents to recording medium

Patent Assignee: SONY CORP (SONY)

Inventor: HIDACHI A; HITACHI A; KAZAMI S; OTA O; TSUCHIDA Y

| Patent Family (3 patents, 33 countries) | | | | | | | |
|---|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| EP 1418581 | A2 | 20040512 | EP 200325486 | A | 20031106 | 200440 | B |
| JP 2004165855 | A | 20040610 | JP 2002327441 | A | 20021111 | 200440 | E |
| US 20040151320 | A1 | 20040805 | US 2003700487 | A | 20031105 | 200452 | E |

Abstract:

The apparatus has a structure creating portion for encrypting input contents (11) with different keys and creating a structure for recording the contents on a **recording medium** e.g. **CD** (50). A data output **portion** groups the keys with which the contents have been encrypted and encrypts the grouped keys. The data output portion creates the grouped encrypted keys and... the contents have been encrypted, encrypts grouped keys with a disc key, and creates a key locker. A disc image creating portion creates image data **to** be recorded on a product **CD** with contents of a first session and a second session and the key locker. In accordance with the image data, the CD is produced. Since... .. encrypts grouped keys with a disc key, and creates a key locker. A disc image creating portion creates image data to be recorded on a **product CD** with contents of a first session and a second session and the key locker. In accordance with the image data, the CD is produced. Since... ..

Claims:

structure creating portion for encrypting a plurality of input contents with different keys and creating a structure for recording the plurality of contents on a **recording medium**; and a **data output portion** for grouping the plurality of **keys** with which the plurality of contents have been encrypted, encrypting the grouped keys, creating the grouped encrypted keys, and outputting the plurality of contents in a recordable format to the recording medium in accordance with the **structure created** by the structure creating **portion**, the grouped encrypted keys being output by the data output portion... .. What is claimed is: 1. An authoring apparatus, comprising: a structure creating portion for encrypting a plurality of input contents with different **keys** and creating a structure for recording the plurality of contents **on a recording medium**; and a data output **portion** for grouping the plurality of keys with which the plurality of contents have been **encrypted**, **encrypting** the grouped keys, creating the grouped **encrypted** keys, and outputting the plurality of contents in a recordable format to the recording medium in accordance with the structure created by the structure creating portion, the grouped encrypted keys being output by the data output **portion**.> ...**Basic Derwent Week: EP 200325486**

22/3,K/5 (Item 5 from file: 350)
DIALOG(R)File 350: Derwent WPIX
(c) 2011 Thomson Reuters. All rights reserved.

Digital audio content distribution management method e.g. for music, involves recognizing distributor's identification code to authenticate user for allowing to playback entire compact disk

Patent Assignee: ONG CORP (ONGO-N); ONG L D (ONGL-I)
Inventor: ONG L D

| Patent Family (4 patents, 100 countries) | | | | | | | |
|--|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| US 20030195851 | A1 | 20031016 | US 2002372249 | P | 20020411 | 200375 | B |
| | | | US 2003411986 | A | 20030411 | | |
| WO 2003088561 | A1 | 20031023 | WO 2003US11027 | A | 20030411 | 200380 | E |
| AU 2003221854 | A1 | 20031027 | AU 2003221854 | A | 20030411 | 200436 | E |
| JP 2005522745 | W | 20050728 | JP 2003585351 | A | 20030411 | 200549 | E |
| | | | WO 2003US11027 | A | 20030411 | | |

Abstract:

PC) (114). If the distributor's identification (ID) code is recognized, the user is identified as an authorized person and allowed to playback the entire **CD**, else allowed to play only a limited **portion** of the **CD**... by their amplitude increment per short traversal times exceeding a predetermined level, and are flagged in the audio data file. A distributor or host ID **code** is embedded in the audio data file designating the authorized source or host environment for playback of the audio data file. A vector-decoding-enabled... Basic Derwent Week: 200375

22/3,K/6 (Item 6 from file: 350)
DIALOG(R)File 350: Derwent WPIX
(c) 2011 Thomson Reuters. All rights reserved.

Read-only digital optical disk used in commercial field, has default format that encodes implementation of variable user data format encoding published works encrypted by variable software algorithm

Patent Assignee: MATSUSHITA DENKI SANGYO KK (MATU); MATSUSHITA ELECTRIC IND CO LTD (MATU)
Inventor: HAN Z; NELSON T J; ZOU H

| Patent Family (3 patents, 2 countries) | | | | | | | |
|--|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| JP 2002140869 | A | 20020517 | JP 2001246030 | A | 20010814 | 200250 | B |
| US 20070143863 | A1 | 20070621 | US 2000640360 | A | 20000816 | 200741 | E |
| | | | US 2007676607 | A | 20070220 | | |
| US 7249384 | B1 | 20070724 | US 2000640360 | A | 20000816 | 200749 | E |

Abstract:

A copy-resistant read-only digital **optical disc** having encrypted digital data. The copy-resistant read-only digital **optical disc** includes a digital work, a variable user-data format encoding said digital work after encryption with a variable software algorithm, an implementation of said variable... .. algorithm, and an implementation of said variable user data format encoded in a default format. The encrypted digital data is read on an adaptable digital **optical disc** player, which is adaptable to a user-data format described on said copy-resistant read-only digital **optical disc** made in accordance with this invention. A copy-resistant read-only digital **optical disc** made in accordance with this invention will

provide necessary user-data format information on the disc in a default format, which is always accessible by... ..

Claims:

What is claimed is: 1. An adaptable digital **optical disc** player for reading **encrypted** digital **data**, said player comprising: a mechanism that adapts to a copy-resistant read-only digital **optical disc**; wherein said copy-resistant read-only digital **optical disc** comprises a digital work, a variable software algorithm for **encrypting** said digital work, provided to a processor on said player, where a variable user-**data** format in a **second zone** **encodes** said digital work **encrypted** with said variable software algorithm, and a default format in a **first zone** encodes an implementation of said variable user-data format; wherein said **first zone** is located at an innermost predetermined **section** of said copy-resistant read-only digital **optical disc** and includes said implementation of said variable user-**data** format **encoded** in said default format; a drive which accepts said read-only digital **optical disc** including said **first** and **second zones** including said **encrypted** digital **data** and outputs a channel-signal stream; a controller which generates commands which cause said drive to access said **first** and **second zones** on said read-only digital **optical disc**; a default sequencer which accepts commands from said controller and said channel-signal stream from said drive and returns a data-byte stream in real-time from said read-only digital **optical disc** through said drive and said default sequencer; a multimedia processor which passes user requests from said adaptable digital **optical disc** player to said controller and receives said **encrypted** digital work and an implementation of said variable software algorithm from said controller; a programmable-sequencer which... .. commands and programmable-sequencer instructions from said controller and said channel-signal stream from said drive, and outputs a data-bit stream; a default ECC-**decoder** which accepts commands from said controller and said data-byte stream from said default sequencer; a programmable ECC-**decoder** which accepts programmable ECC-**decoder** commands and instructions from said controller and said data-bit stream from said programmable-sequencer; wherein said controller reads said implementation of said user-data format in said default format through said default sequencer and said default ECC-**decoder** into said programmable sequencer into said programmable sequencer and reads said implementation of said algorithm and said encrypted digital work through said programmable sequencer and said programmable ECC **decoder**; wherein said programmable-sequencer comprises: a programmable channel-bit converter which accepts channel configuration data from said controller and said channel-signal stream from said... Basic Derwent Week: 200250

22/3,K/7 (Item 7 from file: 350)

DIALOG(R)File 350: Derwent WPIX

(c) 2011 Thomson Reuters. All rights reserved.

Unique identification method for digital content on digital content player, by receiving first, second and third identifiers, and producing fourth unique identifier based on mathematical combination of identifiers

Patent Assignee: IBM CORP (IBMC); INT BUSINESS MACHINES CORP (IBMC); WISTRON CORP (WIST)

Inventor: DORACK J J; DORAK J J

| Patent Family (12 patents, 30 countries) | | | | | | | |
|--|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| CN 1289100 | A | 20010328 | CN 2000127012 | A | 20000914 | 200158 | B |
| EP 1085443 | A2 | 20010321 | EP 2000308024 | A | 20000914 | 200212 | ETAB |
| CA 2316762 | A1 | 20010317 | CA 2316762 | A | 20000817 | 200159 | E |
| JP 2001160003 | A | 20010612 | JP 2000279877 | A | 20000914 | 200159 | E |
| KR 2001050381 | A | 20010615 | KR 200053161 | A | 20000907 | 200171 | E |
| US 6389403 | B1 | 20020514 | US 1998133519 | A | 19980813 | 200239 | E |
| | | | US 1998177096 | A | 19981022 | | |
| | | | US 1999397419 | A | 19990917 | | |
| KR 444695 | B | 20040818 | KR 200053161 | A | 20000907 | 200481 | E |
| CA 2316762 | C | 20070403 | CA 2316762 | A | 20000817 | 200726 | E |
| CN 100345157 | C | 20071024 | | | | 200830 | E |
| EP 1085443 | B1 | 20080827 | EP 2000308024 | A | 20000914 | 200858 | E |
| DE 60040041 | E | 20081009 | DE 60040041 | A | 20000914 | 200868 | E |
| | | | EP 2000308024 | A | 20000914 | | |
| JP 4347508 | B2 | 20091021 | JP 2000279877 | A | 20000914 | 200970 | E |

Abstract:

algorithm. Two keys are mathematically related, As a result, the data encrypted using one key are undecipherable if the other key is not used. The **owner** of a **key** keeps one key (private key) secret, and, generally distributes the 2nd key (public key). In order to protect transmission of a secret message using a a message, a message owner calculates a message digest (it defines in the bottom) first. Then, a message digest is encrypted using an **owner's** private **key**. A message is distributed with the signature. The receipt side of a message can verify a digital signature by decoding a signature first using a message **owner's** public **key**, and recovering|restoring a message digest. Next, the receipt side calculates the received digest of a message and compares with the recovered|restored digest. When... ...The key 201 is public key or a private key. CLRNHG showing the tooth|gear of a key, for example, a clearing house, shows the **owner** of a **key**. PB in a handle|steering-wheel shows that it is public key, therefore the key 201 is the public key of a clearing house. PV...tool to enable it to produce a series of content 113 for electronic distribution. For example, all the content 113 can be produced from the **track**|truck with which 1 or more **CD** which produces from a series of CDs, or is test|inspected by the content provider 101 was selected. The pre-processing parameter can be automatically...regenerate, if it clicks)- Track|truck name object- Track|truck information object- Track|truck lyric button- Track|truck lyric object- Track|truck artist name object- **Track**|truck credit button- **Track**|truck credit object- **CD** name object- **CD** credit button- **CD** credit object- General purpose (configurable) metadata button- General purpose metadata object, othersThe following is contained in the function of the end user...system of an end user. Grouping of music similar to physical CD is stored as a reproduction list. In some cases, a reproduction list emulates **CD** correctly. (For example, when all the **track**|trucks of commercially available **CD** are purchased from the electronic digital content store 103 as an online edition of CD and are defined by the reproduction list equivalent to the...follows (It respond|corresponds to Screen 1601 of an end user interface.)- Reproduction|regeneration- Pause- Stop- It skips back.- It skips to front.- Volume control- **Track**|truck position adjusting- Lyric display- Credit display- **CD** cover display- Artist picture display- Presenting of **track**|truck information- Display of other metadata- Website visit- Reproduction list- Librarian, othersthe inside of implicitness when a digital content librarian digital content librarian selects music... Basic Derwent Week: 200158

Copy protection arrangement in optical disk, utilizes title identifier code and classification code to control recorder to prohibit from making further copies

Patent Assignee: EASTMAN KODAK CO (EAST)

Inventor: ASHE P R

| Patent Family (1 patents, 1 countries) | | | | | | | |
|--|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| US 6070799 | A | 20000606 | US 199734654 | P | 19970108 | 200040 | B |
| | | | US 1997902473 | A | 19970729 | | |

Abstract:

NOVELTY - Optical disk (10) has a title identifier (ID) **code** to identify digital data, and classification **code**. Disk reader (30) reads and indicates the **code** and title ID to process and memory circuit (42). A recorder (31) controlled by processing unit, prohibits from making further copies, and permits to make only single copy from original disk, or does not restrict number of copies to be made by the **code**. USE - Used for limiting the number of copies of recorded data during recording information from original disk to another disk such as DVD , CD-ROM... ..ADVANTAGE - Makes use of barcode technology for providing copy protection for **recording medium**. Hence prevents unauthorized copies. Copy protection including single copy capability can effectively realized... Copy protection for an original **recordable medium** such as an optical disk having at least one recording surface which records digital information, including the digital information having a title ID **code** which identifies the digital information; and a copy classification **code** for the digital information which indicates to a recorder whether it is prohibited from making copies, permitted to make only a single copy or does...

Claims:

from an original disk having at least one recording surface which has a title ID that identifies the digital information, and having a copy classification **code** for the digital information identified by the title ID which indicates to a recorder whether the recorder is prohibited from making copies, permitted to make only a... .. original or does not restrict the number of copies to be made in a copying session, comprising:(a) means for reading and storing a unique **code** from a bar **code** on the **recordable medium**, the unique **code** identifying the original disk;(b) means for reading the title ID and the copy classification **code** from the original disk and for storing the title ID and the copy classification **code** on the first recordable disk **responsive** to the unique **code**; and(c) means responsive to the unique **code**, the title ID and the copy classification **code** for controlling the recorder including means responsive to the copy classification **code** for preventing the recorder from making a **copy** onto a second recordable disk in the copying session.Basic Derwent Week: 200040

22/3,K/9 (Item 9 from file: 350)

DIALOG(R)File 350: Derwent WPIX

(c) 2011 Thomson Reuters. All rights reserved.

Programmable code system for remotely controlling switching functions - uses multiple channels between transmitter and receiver, for conveying numerical code by infrared signals, for driving remote actuator

Patent Assignee: FERPORT SAS DI BIASSONI & C M (FERP-N)

Inventor: BIASSONI M

| Patent Family (2 patents, 25 countries) | | | | | | | |
|---|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| EP 889453 | A2 | 19990107 | EP 1998111928 | A | 19980627 | 199906 | B |
| IT 1297272 | B | 19990809 | IT 1997MI1572 | A | 19970703 | 200170 | E |

Abstract:

The code is assembled hierarchically from plural partial codes, e.g. a **producer code**, set by encoder

(30), a **distributor code**, set by encoder (40), an installer code, set by encoder (50), an end-user personal code, set by encoder (60). The partial codes are assembled...

Claims:

said) at least one encoding devices (30, 40, 50, 60) being adapted to supply to and store into said transmitter (10) and receiver (20) a **portion** or partial code (Cp, **Cd**, Ci, Cu) of said **enabling code** (CODE). ... Basic Derwent Week: 199906...

22/3,K/10 (Item 10 from file: 350)

DIALOG(R)File 350: Derwent WPIX

(c) 2011 Thomson Reuters. All rights reserved.

Digital writing object distributing system for e.g. software, electronic publication used in CD-ROM, network environment - has terminal equipment to read and write information on memory medium at predetermined storing place identified by identification code

Patent Assignee: HITACHI LTD (HITA)

Inventor: SANO K; YAGAWA Y

| Patent Family (2 patents, 2 countries) | | | | | | | |
|--|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| JP 10021144 | A | 19980123 | JP 1996172720 | A | 19960703 | 199814 | B |
| US 6751598 | B1 | 20040615 | US 1997887251 | A | 19970702 | 200439 | E |

Abstract:

digital content updating unit of the terminal system transmits to a distributor a request for transmission of the digital content together with a user profile **code**. The **distributor** refers to a **user** management file to check the validity of the user profile code and the number of times of distribution. If they are valid, the latest edition... ..

Claims:

content, comprising: a drive unit for making an access to information in a storage medium mounted thereto, the storage medium having a read only storage **area** and a **rewritable** storage **area**; a digital content **access** permitting **section**, including a judging section connected to said drive unit for reading a code from a predetermined location on said storage medium and judging whether or... Basic Derwent Week: 199814

28/3,K/1 (Item 1 from file: 350)

DIALOG(R)File 350: Derwent WPIX

(c) 2011 Thomson Reuters. All rights reserved.

Computer system for converting video information from uncompressed format to desired format, has memory for storing application having codes for processing raw video information and performing disk authoring operation

Patent Assignee: MEDIOSTREAM INC (MEDI-N)

Inventor: HUANG Q

| Patent Family (1 patents, 1 countries) | | | | | | | |
|--|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| US 20110044661 | A1 | 20110224 | US 2010907939 | A | 20101019 | 201118 | B |
| | | | US 2007847190 | A | 20070829 | | |
| | | | US 2006342280 | A | 20060127 | | |
| | | | US 2002202999 | A | 20020723 | | |

Abstract:

NOVELTY - Memory e.g. RAM (870) stores integrated software application having code to resize raw

video information to size **associated** with desired output media format. A disk **authoring code** for multiplexing elementary video stream into desired output media format and TV standard, to obtain video and audio information in presentation format is stored in... raw video information in uncompressed format to frame rate associated with desired TV standard is stored in memory. An INDEPENDENT CLAIM is included for computer **recordable medium** for storing program for converting video information... Basic Derwent Week: 201118...

28/3,K/3 (Item 3 from file: 350)
 DIALOG(R)File 350: Derwent WPIX
 (c) 2011 Thomson Reuters. All rights reserved.

Information providing apparatus for distribution of music, video data, compares encryption data using authentication key with received encryption data

Patent Assignee: SONY CORP (SONY)

Inventor: HISAMATSU F; UENO S; YAMANAKA Y; YOSHINO K; YOSHITOMI K

| Patent Family (5 patents, 2 countries) | | | | | | | |
|--|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| JP 2003069558 | A | 20030307 | JP 2001251588 | A | 20010822 | 200338 | B |
| US 20030079042 | A1 | 20030424 | US 2002223798 | A | 20020820 | 200338 | E |
| US 20060185022 | A1 | 20060817 | US 2002223798 | A | 20020820 | 200655 | E |
| | | | US 2006405983 | A | 20060418 | | |
| US 7328458 | B2 | 20080205 | US 2002223798 | A | 20020820 | 200812 | E |
| JP 4151246 | B2 | 20080917 | JP 2001251588 | A | 20010822 | 200863 | E |

Claims:

A recording means to record content data memorize|stored in the memory|storage means on an external storage **medium**; Information **recording** management means which manages operation|movement of the said recording means; 1st internal certification|authentication means to certify|authenticate whether the said content data is... content key with a root key (Kroot); the authoring device including: means for receiving the content identifier (CID), authoring key enabling key (CEK) and the **authoring key** (CED) from the **authoring key** generator; means for storing content **corresponding** to the content identifier (CID); means for storing the content identifier (CID), authoring key enabling key (CEK) and the authoring key (CED); means for decrypting... Basic Derwent Week: 200338

28/3,K/5 (Item 5 from file: 350)
 DIALOG(R)File 350: Derwent WPIX
 (c) 2011 Thomson Reuters. All rights reserved.

Digital signature calculation system for securing program codes, obtains digital signature for signature target data from calculated partial signatures, using secret key of program code owner

Patent Assignee: NEC CORP (NIDE)

Inventor: OBANA M; OBANA S

| Patent Family (4 patents, 2 countries) | | | | | | | |
|--|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| US 20010016911 | A1 | 20010823 | US 2001760805 | A | 20010117 | 200158 | B |
| JP 2001202012 | A | 20010727 | JP 20009037 | A | 20000118 | 200158 | E |
| JP 3584831 | B2 | 20041104 | JP 20009037 | A | 20000118 | 200472 | E |
| US 7103775 | B2 | 20060905 | US 2001760805 | A | 20010117 | 200660 | E |

Claims:

a network; and remote hosts in the network which can be visited by the mobile agent, wherein: the base host includes: an agent execution environment **corresponding** to the **base** host for letting the mobile agent execute its program code; a random number generation means for generating random numbers; a partial signature auxiliary data generation means to which the random numbers generated by the random number generation means and a secret **key** of the **owner** of the mobile **agent** are inputted and which generates partial signature auxiliary data for distributing the information of the secret key of the owner of the mobile agent to... .. calculation for the partial signature auxiliary data generated by the partial signature auxiliary data generation means, and each remote host includes: an agent execution environment **corresponding** to the remote host for **letting** the mobile **agent** execute its program code; a partial signature calculation means to which signature target data, the signature target data being target data to which a digital... Basic Derwent Week: 200158

28/3,K/8 (Item 8 from file: 350)

DIALOG(R)File 350: Derwent WPIX

(c) 2011 Thomson Reuters. All rights reserved.

Intelligent TV system for satellite broadcasting - outputs non-changing image codes such that complete non- changing image shifting occurs during modification of changing image according to camera position to obtain narrow bandwidth signals

Patent Assignee: BRUMMETT P L (BRUM-I)

Inventor: BRUMMETT P L

| Patent Family (1 patents, 1 countries) | | | | | | | |
|--|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| US 5861905 | A | 19990119 | US 1996700850 | A | 19960821 | 199911 | B |

Abstract:

facilitates usage in remote imaging. A high definition sound and image signals is generated by transmitting them in narrow bandwidth line. The data for broadcast, **CD** and other data is retrieved easily from the data stream packets. DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of intelligent camera and...

Claims:

said signals from said microphone means to said camera means and said camera processor means, said camera means including in said digital image codes, a **corresponding** sound code for said image; **studio** processor **means** having an operator input device for manipulating the digital **codes** generated by the camera processor means, said studio processor means separating the non-changing digital codes and changing image codes, identifying the non-changing codes... Basic Derwent Week: 199911

28/3,K/9 (Item 9 from file: 350)

DIALOG(R)File 350: Derwent WPIX

(c) 2011 Thomson Reuters. All rights reserved.

Files protection method e.g. for optical writable disk - having storage layer which is capable of being disrupted when laser beam of sufficient intensity is focused with disk having transparent substrate layer on one side of storage layer and lacquer layer on other side

Patent Assignee: EASTMAN KODAK CO (EAST)

Inventor: BROWNSTEIN S A; CUSHMAN T R; KLINE P J; LENTZ J P

| Patent Family (1 patents, 1 countries) | | | | | | | |
|--|------|----------|--------------------|------|----------|--------|------|
| Patent Number | Kind | Date | Application Number | Kind | Date | Update | Type |
| US 5706266 | A | 19980106 | US 1991810976 | A | 19911220 | 199808 | B |
| | | | US 1992999626 | A | 19921231 | | |
| | | | US 1995432445 | A | 19950501 | | |

Abstract:

The method involves physically embedding an identification signal group in a writable **optical disk**. A second identification signal group is stored in a file written on the writable **optical disk**. On initiation of interaction between an interaction system and the writable **optical disk**, a representation of the two identification **signal** groups is transferred to a **signal** processing unit of the interaction system. The two **identification signals** group representation in the **signal** processing unit and continuing interaction are **compared** between the interaction system and the writable **optical disk** only when the **comparison** between the two **identification signal** group representations is positive... ...A transferred file is decoded prior to processing by the processing unit. Where the interaction system has a third identification **signal** group associated with it, the method involves transferring a representation of the third **identification signal** group to the **signal** processing unit of the interaction system. The third and first **identification signal** group representations are **compared** in the **signal** processing unit. Continuing interaction between the interaction system and the writable **optical disk** only when the **comparison** between the first and third **identification signal** group representations is positive... disruptions provided by the laser beam are selected to provide human readable and/or machine readable patterns. To reduce the damage to portions of the **optical disk** other than the **storage** layer, the storage layer is exposed to the laser beam prior to curing, or prior to applying and curing the lacquer layer. The **optical disk** can be of the type with data written thereon during fabrication, or the disk can be of the type in which data can be impressed thereon after fabrication of the **optical disk**. The patterns on the **optical disk** can be in the form of optical bar codes. In one application of the present invention involving the type of disk on which data can be written after fabrication...

Claims:

A method of protecting files stored on an **optical** writable **disk**, said method comprising the steps of: physically embedding a **first identification signal** group in a writable **optical disk**; storing a **second identification signal** group in a file written on said writable **optical disk**; on initiation of interaction **between an** interaction system and said writable **optical disk**, transferring a representation of said first **and said second identification** signal group to a signal processing unit of said interaction system; **comparing** said **first** and said **second identification signal** group representation in said signal processing... ... wherein said interaction system has a third identification signal group associated therewith, said method further comprising the steps of transferring a representation of said third **identification** signal group to the signal processing unit of said interaction system and **comparing** said third and first **identification signal** group representations in said **signal** processing unit **and** continuing interaction between said **interaction system** and said writable optical **disk** only when said **comparison** between said first and third **identification signal** group representations is positive. Basic Derwent Week: 199808

28/3,K/11 (Item 11 from file: 347)

DIALOG(R)File 347: JAPIO

(c) 2011 JPO & JAPIO. All rights reserved.

DRIVING MECHANISM FOR OPTICAL HEAD FOR OPTICAL DISC

Pub. No.: 57-167147 [JP 57167147 A]

Published: October 14, 1982 (19821014)

Inventor: OGOSHI SEIICHI

Applicant: TOSHIBA CORP [000307] (A Japanese Company or Corporation), JP (Japan)

Application No.: 56-053539 [JP 8153539]

Filed: April 09, 1981 (19810409)

Journal: Section: P, Section No. 168, Vol. 07, No. 10, Pg. 67, January 14, 1983 (19830114) ...

Published: 19821014)

ABSTRACT:

CONSTITUTION: A magnetic circuit 22 is formed which has comparatively wide magnetic gaps 21 extending in the direction of the radius of a disc-shaped **recording medium** (which is not shown in figure) and is closed in the terminal in the direction of the radius, and movable yokes 23 having a length... ...arranged in magnetic gaps 21. Partially narrow gaps 24 are formed, and AFC driving coils

25 for an optical head, ATC driving coils 26, and **ASC** driving coils 27 are provided in **relation** to these movable yokes 23. Movable yokes 23 move in accordance with the movement of the optical head in the direction of the radius to... Di01

DIALOG(R)File 348: EUROPEAN PATENTS
(c) 2011 European Patent Office. All rights reserved.
19/3K/5 (Item 5 from file: 348)

Optical disk apparatus, optical disk recording method, and optical disk

Patent Assignee:

- **Sony Corporation** (100224958)
7-35, Kitashinagawa 6-chome Shinagawa-ku; Tokyo (JP)
(Proprietor designated states: all)

Inventor:

- **Kobayashi, Seiji**
c/o Sony Corporation,7-35, Kitashinagawa 6-chome; Shinagawa-ku,Tokyo; (JP)
- **Ito, Kazumine**
c/o Sony Corporation,7-35, Kitashinagawa 6-chome; Shinagawa-ku,Tokyo; (JP)
- **Horigome, Toshihiro**
c/o Sony Corporation,7-35, Kitashinagawa 6-chome; Shinagawa-ku,Tokyo; (JP)

Legal Representative:

- **Melzer, Wolfgang et al (100004085)**
Mitscherlich & Partner Patent- und Rechtsanwälte Postfach 33 06 09; 80066 Munchen; (DE)

| | Country | Number | Kind | Date | |
|-------------|---------|------------|------|----------|---------|
| Patent | EP | 1162615 | A2 | 20011212 | (Basic) |
| Patent | EP | 1162615 | A3 | 20040519 | |
| Patent | EP | 1162615 | B1 | 20100901 | |
| Application | EP | 2001113898 | | 20010607 | |
| Priorities | JP | 2000175574 | | 20000607 | |

Specification:

1D are schematic diagrams for explaining a mini disk used in the present invention;
Fig. 2 is a flowchart showing a process of manufacturing the **mini disk** in Fig. 1;
Fig. 3 is a **block** diagram showing a bar **code writer** in an embodiment of the present invention;
Fig. 4 is a block diagram showing a 4-1 modulator in the bar **code writer** of Fig. 3;
Fig. 5 is a **block** diagram showing an **optical disk** apparatus to access the **mini disk** of Fig. 1;
Fig. 6 is a **block** diagram showing a second decoder in the **optical disk** apparatus of Fig. 5; and
Fig. 7 is a block diagram showing a maximum detector in the second decoder of Fig. 6.
DETAILED DESCRIPTION OF... ..next step in the optical disk manufacturing process 1, the copyright protective information ED outputted from a signal source 16 is recorded by a bar **code writer** 18, and subsequently the mini disk 2 is packaged and shipped. The bar **code writer** 18 modulates a high-output laser beam, which is emitted from a YAG (yttrium aluminum garnet) laser or the like, with the copyright protective information ED and then irradiates the modulated beam to an inner **area** of the **mini disk** 2 to change the information recording plane of the mini disk 2 locally and unreversibly by the copyright protective information ED, thereby recording the copyright protective information ED. At

this time, the bar **code writer** 18 records the copyright protective information ED by irradiating a laser beam which is radially long and narrow in shape, thereby recording the copyright protective information ED like a bar code in a predetermined inner **area** of the **mini disk** 2. In this stage, the bar **code writer** 18 unreversibly changes the information recording film, which is composed of a reflective film, by irradiation of the laser beam to thereby unreversibly change the... ..2 containing the copyright protective information ED recorded as mentioned. The copyright protective information ED is recorded like a bar code in a predetermined inner **area** ARED of the **mini disk** 2. The **area** ARED for recording the copyright protective information ED is set to 0.8 mm in width around a diameter of 22.1 mm. The copyright...

DIALOG(R)File 348: EUROPEAN PATENTS
(c) 2011 European Patent Office. All rights reserved.
19/3K/6 (Item 6 from file: 348)

System and method for processing protected data

Patent Assignee:

- **Sony Corporation** (214029)
6-7-35 Kitashinagawa, Shinagawa-ku; Tokyo 141 (JP)
(Applicant designated States: all)

Inventor:

- **Nonaka, Akira, Sony Corp., Intel. Prop. Dep.**
6-7-35 Kitashinagawa, Shinagawa-ku; Tokyo 141; (JP)
- **Ezaki, Tadashi, Sony Corp., Intel. Prop. Dep.**
6-7-35 Kitashinagawa, Shinagawa-ku; Tokyo 141; (JP)

Legal Representative:

- **Pilch, Adam John Michael et al (50481)**
D Young & Co 120 Holborn; London EC1N 2DY; (GB)

| | Country | Number | Kind | Date | |
|-------------|---------|------------|------|----------|---------|
| Patent | EP | 1130492 | A2 | 20010905 | (Basic) |
| Patent | EP | 1130492 | A3 | 20041110 | |
| Application | EP | 2000311199 | | 20001214 | |
| Priorities | JP | 99361225 | | 19991220 | |

Specification:

and the signature data SIG1,ESC)) therefor, which are shown in Figs. 3B and 3C, stored in the securecontainer 104 recorded on the secure RAM **area** 132 of the **recording medium** (ROM) 1301)), are written into the work memory 200 via the medium drive SAM manager 855. In step S51-3, after verifying the integrity of... ..KCP,P)). The signature processor 189 also verifies the integrity of the signature data SIGK1,ESC)) stored in the key file KF, i.e., the **creator** of the **key** file KF, by using the public key data KESC,P)) read from the storage unit 192. Subsequently, in step S51-4, after verifying the integrity...

DIALOG(R)File 348: EUROPEAN PATENTS
(c) 2011 European Patent Office. All rights reserved.
19/3K/7 (Item 7 from file: 348)

CONTENTS MANAGEMENT SYSTEM, DEVICE, METHOD, AND PROGRAM STORAGE MEDIUM

Patent Assignee:

- **Sony Corporation** (214028)
7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001 (JP)
(Applicant designated States: all)

Inventor:

- **ISHIBASHI, Yoshihito, Sony Corporation**
7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)
- **OHSHI, Tateo, Sony Corporation**
7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)
- **MUTO, Akihiro, Sony Corporation**
7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)
- **KITAHARA, Jun, Sony Corporation**
7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)
- **SHIRAI, Taizou, Sony Corporation**
7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)

Legal Representative:

- **DeVile, Jonathan Mark, Dr. et al (91151)**
D. Young & Co 21 New Fetter Lane; London EC4A 1DA; (GB)

| | Country | Number | Kind | Date | |
|-------------|---------|------------|------|----------|---------|
| Patent | EP | 1128598 | A1 | 20010829 | (Basic) |
| | WO | 200119017 | | 20010315 | |
| Application | EP | 2000956997 | | 20000907 | |
| | WO | 2000JP6089 | | 20000907 | |
| Priorities | JP | 99253660 | | 19990907 | |
| | JP | 99253661 | | 19990907 | |
| | JP | 99253662 | | 19990907 | |
| | JP | 99253663 | | 19990907 | |
| | JP | 99260638 | | 19990914 | |
| | JP | 99264082 | | 19990917 | |
| | JP | 99265866 | | 19990920 | |

Specification:

time, supplies the information on profit distribution, and receives information (a handling policy) to be attached to the contents, if necessary. A copying right management **section** 13 transmits information indicating results of content utilization of the user home network 5 to an organization managing copying rights, e.g., JASRAC (Japanese Society for Rights of **Authors**, Composers and Publishers). A key server 14 performs generation, maintenance, management of keys used for the entire system, and the individual key KI)) different for...supplied to an authentication station 22, if necessary, and the delivery key Kd)) is supplied to the user home network 5 via a user management **section** 18. In addition, a public key and a secret key of the electronic distribution center 1 as well as a public key and a secret...

DIALOG(R)File 348: EUROPEAN PATENTS
(c) 2011 European Patent Office. All rights reserved.
19/3K/8 (Item 8 from file: 348)

Recording medium, method and apparatus for producing recording medium and data recording method and apparatus

Patent Assignee:

- **SONY CORPORATION (214024)**
7-35, Kitashinagawa 6-chome Shinagawa-ku; Tokyo (JP)
(Applicant designated States: all)

Inventor:

- **Furukawa, Shunsuke**
c/o Sony Corporation, 7-35, Kitashinagawa 6-chome; Shinagawa-ku, Tokyo; (JP)
- **Sako, Yoichiro**
c/o Sony Corporation, 7-35, Kitashinagawa 6-chome; Shinagawa-ku, Tokyo; (JP)

Legal Representative:

- **Nicholls, Michael John (61941)**
J.A. KEMP & CO. 14, South Square Gray's Inn; London WC1R 5JJ; (GB)

| | Country | Number | Kind | Date | |
|-------------|---------|------------|------|----------|---------|
| Patent | EP | 1081698 | A2 | 20010307 | (Basic) |
| Patent | EP | 1081698 | A3 | 20030423 | |
| Application | EP | 2000307442 | | 20000830 | |
| Priorities | JP | 99246549 | | 19990831 | |

Specification:

generate a key. The information converted from the sector addresses 128, 129, 130, (center dot)(center dot)(center dot), 32766, 32767 is recorded in the **area 5** of the disc-shaped **recording medium 1**. Meanwhile, in the disc-shaped recording medium 1, an encryption key may be recorded in a pre-set **area** for address data of the disc-shaped **recording medium 1**, such as in a **sector 127**. If data including main data is recorded in the pre-set area by a data recording apparatus, as later explained, an encryption key may also be recorded in the data sector. Moreover, a **code** of a **producer** of the disc-shaped recording medium or an ID of the disc-shaped recording medium 1 may be substituted for part or all of the...

DIALOG(R)File 348: EUROPEAN PATENTS
(c) 2011 European Patent Office. All rights reserved.
19/3K/15 (Item 15 from file: 348)

Method and system for digitally compensating for film unit defects

Patent Assignee:

- **EASTMAN KODAK COMPANY** (201212)
343 State Street; Rochester, New York 14650 (US)
(Applicant designated States: all)

Inventor:

- **Smart, David C., c/ o Eastman Kodak Co.**
Patent Legal Staff, 343 State Street; Rochester, New York 14650-2201; (US)
- **Cipolla, David, c/ o Eastman Kodak Co.,**
Patent Legal Staff, 343 State Street; Rochester, New York 14650-2201; (US)

Legal Representative:

- **Weber, Etienne Nicolas et al (91684)**
Kodak Industrie, Departement Brevets, CRT, Zone Industrielle; 71102 Chalon sur Saone
Cedex; (FR)

| | Country | Number | Kind | Date | |
|-------------|---------|----------|------|----------|---------|
| Patent | EP | 1016923 | A2 | 20000705 | (Basic) |
| Patent | EP | 1016923 | A3 | 20040128 | |
| Application | EP | 99204204 | | 19991208 | |
| Priorities | US | 221420 | | 19981228 | |

Specification:

10 and a single associated logical memory unit 20. Unique identifiers 42 can be readily provided by use of non-repeating sequences of numbers or **codes**. If different **producers** are likely to use the same numbers, then it is also desirable that producer identification also be included in the identifiers 42 to ensure uniqueness. The identifier 42 is printed on a film unit 10 or recorded in some other manner, such as digital recording on an **area** of magnetic or optical **recording media**. The identifier 42 is human or machine-readable or both prior to exposure of images. It is preferred that the identifier 42 be recorded independently...

DIALOG(R)File 348: EUROPEAN PATENTS
(c) 2011 European Patent Office. All rights reserved.
19/3K/21 (Item 21 from file: 348)

Recording medium having text information recorded in a plurality of subcode channels and reproducing apparatus

Patent Assignee:

- **SONY CORPORATION** (214024)
7-35, Kitashinagawa 6-chome Shinagawa-ku; Tokyo (JP)
(Proprietor designated states: all)

Inventor:

- **Yokota, Teppei, c/ o Sony Corp.**
7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo; (JP)

Legal Representative:

- **Melzer, Wolfgang, Dipl.-Ing. et al (8278)**
Patentanwalte Mitscherlich & Partner, Sonnenstrasse 33; 80331 Munchen; (DE)

| | Country | Number | Kind | Date | |
|-------------|---------|----------|------|----------|---------|
| Patent | EP | 791925 | A2 | 19970827 | (Basic) |
| Patent | EP | 791925 | A3 | 19990519 | |
| Patent | EP | 791925 | B1 | 20011114 | |
| Application | EP | 96115085 | | 19960919 | |
| Priorities | JP | 95244959 | | 19950922 | |

Claims:

of the program information recorded in the program area, a classification of the program information recorded in the program area, and a name of a **producer**; a **code** determining whether or not the letter information associated with each program information type recorded in the program **area** can be copied on another **recording medium**; a code identifying a conversion code format of the letter information associated with each program information type recorded in the program area; a code identifying... decoding; and display means (58) for displaying the decoded character information from the decoding means.

18. The system as claimed in claim 17, wherein management **area** of the disc-shaped **recording medium** is recorded with a plurality of identifiers for identifying the type of the character information, the plurality of identifiers including at least three of the... ..of the program information recorded in the program area, a classification of the program information recorded in the program area, and a name of a **producer**; a **code** determining whether or not the character information associated with each program information type recorded in the program **area** can be copied on another **recording medium**; a code identifying a conversion code format of the character information associated with each program information type recorded in the program area; a code identifying... ..of the program information recorded in the program area, a classification of the program information recorded in the program area, and a name of a **producer**; a **code** determining whether or not the character information associated with each program information type recorded in the program **area** can be copied on another **recording medium**; a code identifying a conversion code format of the character information associated with each program information type recorded in the program area; a code identifying...

DIALOG(R)File 348: EUROPEAN PATENTS
(c) 2011 European Patent Office. All rights reserved.
19/3K/22 (Item 22 from file: 348)

Compact disc player security system reproducing method and apparatus

Patent Assignee:

- **Sony Computer Entertainment Inc. (3064090)**
7-1-1 Akasaka, Minato-ku; Tokyo 107-0052 (JP)
(Proprietor designated states: all)

Inventor:

- **Kutaragi, Ken, c/ o Sony Corporation**
7-35, Kitashinagawa 6-chome; Shinagawa-ku, Tokyo; (JP)
- **Hirano, Tetsuya, c/ o Sony Corporation**
7-35, Kitashinagawa 6-chome; Shinagawa-ku, Tokyo; (JP)

Legal Representative:

- **Muller, Frithjof E., Dipl.-Ing. et al (8661)**
Patentanwalte MULLER & HOFFMANN, Innere Wiener Strasse 17; 81667 Munchen; (DE)

| | Country | Number | Kind | Date |
|-------------|---------|----------|------|------------------|
| Patent | EP | 723216 | A2 | 19960724 (Basic) |
| Patent | EP | 723216 | A3 | 19960904 |
| Patent | EP | 723216 | B1 | 20010620 |
| Application | EP | 95118162 | | 19951117 |
| Priorities | JP | 94285390 | | 19941118 |

Specification:

ROM disc and security check method for the same. A security code is recorded in a predetermined code region in a sector of a boot **sector** in the innermost **track** of the **CD** ROM disc. The security code indicates that the CD ROM disc is duly licensed, namely by a television game machine **producer**. The security **code** further may contain a program to be executed after a checking operation of the security code. This document does not disclose a special modulation scheme...

19/3K/23 (Item 23 from file: 349)
DIALOG(R)File 349: PCT FULLTEXT
(c) 2011 WIPO/Thomson. All rights reserved.

RECORDING MEDIUM, APPARATUS FOR FORMING THE RECORDING MEDIUM, AND APPARATUS AND METHOD FOR REPRODUCING THE RECORDING MEDIUM**Patent Applicant/ Patent Assignee:**

- **LG ELECTRONICS INC**
20, Yoido-dong, Youngdungpo-gu, Seoul 150-010; KR; KR(Residence); KR(Nationality); (For all designated states except: US)

Patent Applicant/ Inventor:

- **KIM Jin Yong**
109-602, Seonkyung Apt., Yatap-dong, Bundang-gu, Seongnam, Kyunggi-do 463-928; KR; KR(Residence); KR(Nationality); (Designated only for: US)
- **SUH Sang Woon**
110-709, Hyundai Apt., 1346, Seocho 2-dong, Seocho-gu, Seoul 137-861; KR; KR(Residence); KR(Nationality); (Designated only for: US)

Legal Representative:

- **PARK Lae Bong (agent)**
1 Fl., Dongun Bldg., 413-4, Dogok 2-dong, Kangnam-gu, Seoul 135-272; KR

| | Country | Number | Kind | Date |
|-------------|---------|------------|------|----------|
| Patent | WO | 200475193 | A1 | 20040902 |
| Application | WO | 2004KR338 | | 20040219 |
| Priorities | US | 2003447706 | | 20030219 |

| | Country | Number | Kind | Date |
|--|---------|---------------|------|----------|
| | KR | 1020030073800 | | 20031022 |

Detailed Description:

etc. being included in outputted main 15 data. However, where the control data is not legal or there is no control data in the contents **authoring code** file, the CPCC generates and outputs control data containing a CPI flag fixed at 'CPI-Flag=I' and wrong CPI or no CPI. In particular... ..the generated CSI being included in the outputted control data and the others being included in the outputted main data, respectively. Fig. 10 is a **block** diagram showing the configuration of an **optical disc** device for reproducing the BD-ROM according to the second embodiment of the present invention while judging whether it is an illegally copied disc. As...

19/3K/25 (Item 25 from file: 349)

DIALOG(R)File 349: PCT FULLTEXT

(c) 2011 WIPO/Thomson. All rights reserved.

SYSTEM FOR MANAGING DISTRIBUTION OF DIGITAL AUDIO CONTENT

Patent Applicant/ Patent Assignee:

- **ONG CORP**
481 Hackensack Avenue, Hackensack, NJ 07601; US; US(Residence); US(Nationality)

Inventor(s):

- **ONG Lance D**
481 Hackensack Avenue, Hackensack, NJ 07601; US

Legal Representative:

- **CHONG Leighton K (agent)**
Ostrager Chong & Flaherty (Hawaii), 841 Bishop Street, Suite 1200, Honolulu, HI 96813; US

| | Country | Number | Kind | Date |
|-------------|---------|-------------|------|-----------------|
| Patent | WO | 200388561 | A1 | 20031023 |
| Application | WO | 2003US11027 | | 20030411 |
| Priorities | US | 2002372249 | | 20020411 |

Detailed Description:

number of times on any compatible (vector-decoding-enabled) player having firmware enabling playback of the vector-encoded audio file, indicated at Block 111. A **distributor ID code** may be used initially in place of a host-ID code, and is recognized by the player as permitting full playback of the audio file from the CD. However, when the vector-encoded audio file is copied ("ripped") from the **CD**, at **Block 112**, or down loaded from the Internet, at Block 113, to a host environment, such as a personal computer (PC) indicated... ..audio file before playback, at Block 116. If the audio file has been loaded from a legitimately purchased CD, the WaveTrace player checks for the **distributor's ID code**, at Block 117. If the distributor's ID code is recognized, the WaveTrace player changes it to a host-ID code identifying the user as...

IMPROVEMENTS RELATING TO SECURITY IN DIGITAL DATA DISTRIBUTION

Patent Applicant/ Patent Assignee:

- **CERBERUS CENTRAL LIMITED**
2 Princes Street, London W1R 7RA; GB; --(Residence); --(Nationality); (For all designated states except: US)

Patent Applicant/ Inventor:

- **FARIA Richard**
Cerberus Central Limited, 2 Princes Street, London W1R 7RA; GB; GB(Residence); GB(Nationality); (Designated only for: US)

Legal Representative:

- **AHMAD Sheikh Shakeel(et al)(agent)**
David Keltie Associates, Fleet Place House, 2 Fleet Place, London EC4M 7ET; GB

| | Country | Number | Kind | Date |
|-------------|---------|------------|-------|----------|
| Patent | WO | 200379349 | A2-A3 | 20030925 |
| Application | WO | 2003GB1085 | | 20030314 |
| Priorities | GB | 20026034 | | 20020314 |
| | GB | 200211134 | | 20020515 |

Detailed Description:

CD formats can be found at the following web site. www.ee.washington.edu/conselec/CE/k-uhn/cdaudio2/95x7.htm. The audio on a **CD** is divided into a maximum of 99 **tracks**. Each track must be at least four seconds in length, and a pause of two seconds may be inserted between tracks. The audio may be... ..should be included to identify that track uniquely. The ISRC comprises 12 characters divided as shown in the table below.

Length (chars) Description

2 Country **code**

3 First **owner** (allocated by Phonographic Performance Ltd for audio)

2 Year of recording (the last two digits)

5 Designation code (...a table of contents (TOC). The TOC usually includes the timecode for each track (as minutes, seconds and sometimes frames) and is used to enable **CD** players to "know" where each **track** is on the **CD**. The TOC may also define the **track** type which, for some **CD** formats, can be audio or data. In addition to the main data channel (which may contain audio or other, data), there are eight subcode channels...

METHOD AND DEVICE FOR DATA TRANSFER TO AND FROM A CD

Patent Applicant/ Patent Assignee:

- **DOC WITNESS LTD**
8 Hamelacha Street, Rish Haayin 48091; IL; IL(Residence); IL(Nationality); (For all designated states except: US)

Patent Applicant/ Inventor:

- **LOEWIDT Amos**
8 Hamelacha Street, 48091 Rosh Haayin; IL; IL(Residence); IL(Nationality); (Designated only for: US)

Legal Representative:

- **FRIEDMAN Mark M (agent)**
Beit Samueloff, 7 Haomanim Street, 67897 Tel Aviv; IL

| | Country | Number | Kind | Date |
|-------------|---------|-----------|-------|----------|
| Patent | WO | 200341067 | A2-A3 | 20030515 |
| Application | WO | 2002IL889 | | 20021107 |
| Priorities | IL | 146414 | | 20011108 |

Detailed Description:

as a musical CD-ROM, DVD or a soft-ware installation CD-ROM disc. Further pressing of the drive D display icon displays data from **CD ROM area** 160, and initiates an identification process. The computer ...ROM data uploaded into the CPU of the PC directs the PC back to card 100 to locate the necessary validation information including card **owner** passwords, **codes**, and other security tools. The card access control information can also be stored on both the card **CD** or **DVD** ROM recordable **area** 160 as well as chip 102 ROM and RAM and EPROM regions. However, chip 102 cannot be accessed through its electrical contacts of terminal 170...and EPROM areas is enabled through tile input/output region of optical data area 140. As a result Of Start-Lip operating instructions read from **area** 160, the computer **CD** or **DVD** drive reading lens beam is directed to read specific sector of tracks on card 100, which are in effect optical data area 140. Data emission...

19/3K/29 (Item 29 from file: 349)
DIALOG(R)File 349: PCT FULLTEXT
(c) 2011 WIPO/Thomson. All rights reserved.

METHOD FOR STEGA-CIPHER PROTECTION OF COMPUTER CODE**Patent Applicant/ Patent Assignee:**

- **THE DICE COMPANY**

Inventor(s):

- **MOSKOWITZ Scott A**
- **COOPERMAN Marc**

| | Country | Number | Kind | Date |
|--|---------|--------|------|------|
|--|---------|--------|------|------|

| | Country | Number | Kind | Date |
|-------------|---------|----------|------|----------|
| Patent | WO | 9726732 | A1 | 19970724 |
| Application | WO | 97US651 | | 19970116 |
| Priorities | US | 96587943 | | 19960117 |

Claims:

the software which is accessing the watermark where license information consists of one or more of the following items: owning organization name; Personal Owner name; **Owner** Address; License **code**; Software serialization number; Distribution parameters; Appropriate executable general computing device architecture; Pricing; and Software Metering details.

3 The method of claim 1 further comprising the... via a transmission means, from a publisher to a subscriber wherein transmission means can be selected from the group of soft sector magnetic disk media; hard **sector** magnetic disk media; magnetic tape media; **optical disc** media; Digital Video Disk media; magneto-optical disk media; memory cartridge; telephone lines; 16 SCSI; is Ethernet or Token Ring Network; ISDN; ATM network; TCP...

DIALOG(R) File 348: EUROPEAN PATENTS

(c) 2011 European Patent Office. All rights reserved.

25/3K/4 (Item 4 from file: 348)

Method and terminal device for preventing unauthorized use of secured content files

Patent Assignee:

- **Nokia Corporation (2963881)**
Keilalahdentie 4; 02150 Espoo (FI)
(Applicant designated States: all)

Inventor:

- **Rahnasto, Ilkka, J.**
Riekkopolku 3B; 01450 Vantaa; (FI)

Legal Representative:

- **Becker Kurig Straus (101571)**
Patentanwalte Bavariastrasse 7; 80336 Munchen; (DE)

| | Country | Number | Kind | Date | |
|-------------|---------|------------|------|----------|---------|
| Patent | EP | 1890247 | A2 | 20080220 | (Basic) |
| Patent | EP | 1890247 | A3 | 20080917 | |
| Application | EP | 2007020059 | | 20010427 | |
| Priorities | US | 561211 | | 20000428 | |

Specification:

the distributor code for a distributor authorized to distribute the content file and a key code that is formed as a combination of the identification **code** and the **distributor code**. The terminal device needs to have the key code that **matches** the identification **code** and the **distributor code** in order to properly receive and use the content file. The administrator may distribute several key codes each

representing a different content file or a... ..the terminal devices 40 and 60 may be constructed in a similar manner. The data 60 may be a locally-stored medium such as a **CD-ROM**, a magnetic diskette, a tape, etc. or the data may be accessed through a network such as the Internet or the data 60 may...

DIALOG(R)File 348: EUROPEAN PATENTS
(c) 2011 European Patent Office. All rights reserved.
25/3K/5 (Item 5 from file: 348)

Reproducing apparatus and server system providing additional information therefor

Patent Assignee:

- **SAMSUNG ELECTRONICS CO., LTD.** (1093728)
416, Maetan-dong, Paldal-gu; Suwon-City, Kyungki-do (KR)
(Applicant designated States: all)

Inventor:

- **Chung, Hyun-kwon**
104-906 Dongbo Apt. 45, Tanbeol-ri, Gwangju-eup; Gwangju-gun, Gyeonggi-do; (KR)
- **Heo, Jung-Kwon, 203-504 Jugong 2-danji Apt.**
18-1 Banpo 2-dong, Seocho-gu; Seoul; (KR)

Legal Representative:

- **Chugg, David John et al (78311)**
Appleyard Lees, 15 Clare Road; Halifax, West Yorkshire HX1 2HY; (GB)

| | Country | Number | Kind | Date | |
|-------------|---------|------------|------|----------|---------|
| Patent | EP | 1239376 | A2 | 20020911 | (Basic) |
| Patent | EP | 1239376 | A3 | 20050209 | |
| Application | EP | 2001305330 | | 20010619 | |
| Priorities | KR | 201012444 | | 20010310 | |

Specification:

present invention. One or more contents # 1, # 2, ..., and # N and an international standard recording code (ISRC) given to the contents are recorded in an **optical disc 1**, which is a **recording medium** according to the present embodiment. The ISRC code is an international standard code used for distinguishing music, songs, music videos and is given by the Recording Industry **Association** of America (RIAA). The ISRC code includes country **code**, **copyright holder code**, year of recording, and recording number. A reproduction apparatus 10 includes an identifier generator 11, a controller 12, a network connector 13, a reading unit... ..recorded in the storage medium 1. The identifier generated according to the present invention is the ISRC code. The ISRC code is read from the **optical disc 1** by the reading unit 15 and is provided to the identifier generator 11. The network connector 13, which is a connection interface to be...

25/3K/8 (Item 8 from file: 349)
DIALOG(R)File 349: PCT FULLTEXT
(c) 2011 WIPO/Thomson. All rights reserved.

SYSTEM, METHOD AND APPARATUS FOR SECURELY PROVIDING CONTENT VIEWABLE ON A SECURE DEVICE

Patent Applicant/ Patent Assignee:

- **WIDEVINE TECHNOLOGIES INC**
900 Fourth Avenue, Suite 3400, Seattle, WA 98164; US; US(Residence); US(Nationality); (For all designated states except: US)

Patent Applicant/ Inventor:

- **MORTEN Glenn A**
6035 173rd Avenue S.E., Bellevue, WA 98006; US; US(Residence); US(Nationality); (Designated only for: US)

Legal Representative:

- **BRANCH John W(et al)(agent)**
Darby & Darby P.C., P.O. Box 5257, New York, NY 10150-5257; US

| | Country | Number | Kind | Date |
|-------------|---------|------------|-------|----------|
| Patent | WO | 200484035 | A2-A3 | 20040930 |
| Application | WO | 2004US8202 | | 20040316 |
| Priorities | US | 2003455723 | | 20030318 |
| | US | 2004760642 | | 20040120 |

Detailed Description:

variety of content - media II 2, including, but not limited to a DVD, high definition DVD, Video Compact Disc (VCD), Super VCD (SVCD), Super Audio **CD** (SACD), and the like. For example, secure content may be copied and distributed on a Dynamic Digital Sound (DDS) content media. Moreover, distributor 106 may also copy and distribute secure content on a Read/Write **DVD**, **CD**-Recordable (**CD-R**), and substantially similar content media. Distributor 106 is not limited to copying and distributing secure content --WO 2004/084035 PCT/US2004/008202 on **DVD** and **CD** content media technologies, and virtually any other content media technology may be employed without departing from the scope of the present invention.. Distributor 106 may receive one or more screener keys **associated** with the one or more **key** packages. **Distributor** 106 may also receive authorization information from a variety of trusted sources that indicate whether a user has authorization to access the secure content. Provided...

25/3K/15 (Item 15 from file: 349)
DIALOG(R)File 349: PCT FULLTEXT
(c) 2011 WIPO/Thomson. All rights reserved.

METHOD AND APPARATUS FOR SECURE IDENTIFICATION FOR NETWORKED ENVIRONMENTS

Patent Applicant/ Patent Assignee:

- **CK GLOBAL INC**
14211 Livingston, Tustin, CA 92780; US; US(Residence); US(Nationality); (For all designated states except: US)

Patent Applicant/ Inventor:

- **AARONS Michael Thomas**
17299 Flametree Circle, Fountain Valley, CA 92708; US; US(Residence); US(Nationality);
(Designated only for: US)

Legal Representative:

- **ALTMAN Daniel E (agent)**
Knobbe, Martens, Olson & Bear, LLP, 620 Newport Center Drive, 16th Floor, Newport Beach,
CA 92660; US

| | Country | Number | Kind | Date |
|-------------|---------|-------------|-------|----------|
| Patent | WO | 200212983 | A2-A3 | 20020214 |
| Application | WO | 2001US41573 | | 20010806 |
| Priorities | US | 2000223204 | | 20000804 |

Detailed Description:

this manner, the data is kept secure in the event that the invention is lost or stolen. Although the data can be read in any **CD** ROM recorder, encryption keeps the data from being used in a fraudulent manner.

[0019] Prior art, such as credit cards, make use of the **owner's** cursive **signature** to be used in **comparison** to signify proper- and legal-use. -This invention,- in one of its forms, allows the owner's cursive signature to be digitally scanned and stored...

25/3K/16 (Item 16 from file: 349)

DIALOG(R)File 349: PCT FULLTEXT

(c) 2011 WIPO/Thomson. All rights reserved.

METHOD AND TERMINAL DEVICE FOR PREVENTING UNAUTHORIZED USE OF SECURED CONTENT FILES**Patent Applicant/ Patent Assignee:**

- **NOKIA CORPORATION**
Keilalahdentie 4, FIN-02150 Espoo; FI; FI(Residence); FI(Nationality)
- **NOKIA INC**
6000 Connection Drive, Irving, TX 75039; US; US(Residence); US(Nationality); (Designated only for: LC)

Inventor(s):

- **RAHNASTO Iikka J**
Riekkopolku 3B, FIN-01450 Vantaa; FI

Legal Representative:

- **STOUT Donald E(et al)(agent)**
Antonelli, Terry, Stout & Kraus, LLP, Suite 1800, 1300 N. Seventeenth Street, Arlington, VA 22209; US

| | Country | Number | Kind | Date |
|-------------|---------|------------|-------|-----------------|
| Patent | WO | 200184282 | A2-A3 | 20011108 |
| Application | WO | 2001IB702 | | 20010427 |
| Priorities | US | 2000561211 | | 20000428 |

Detailed Description:

the distributor code for a distributor authorized to distribute the content file and a key code that is formed as a combination of the identification **code** and the **distributor code**. The terminal device needs to have the key code that **matches** the identification **code** and the **distributor code** in order to properly receive and use the content file. The administrator may distribute several key codes each representing a different content file or a... ..the terminal devices 40 and 60 may be constructed in a similar manner. The data 60 may be a locally-stored medium such as a **CD-ROM**, a magnetic diskette, a tape, etc. or the data may be accessed through a network such as the Internet or the data 60 may...

NPL Search Results

23/5/2 (Item 2 from file: 8)

DIALOG(R)File 8: Ei Compendex(R)

(c) 2011 Elsevier Eng. Info. Inc. All rights reserved.

Collaborative coding and decoding techniques for multiple access channel

Ali, F.; Honary, B.

Corresp. Author/ Affil: Ali, F.: Lancaster Univ, Lancaster, United Kingdom

IEE Proceedings: Communications (IEE Proc Commun) 1994 141/2 (56-62)

Publication Date: 19940101

Item Identifier (DOI): [10.1049/ip-com:19941043](https://doi.org/10.1049/ip-com:19941043)

Document Type: Article; Journal **Record Type:** Abstract

Language: English **Summary Language:** English

Number of References: 22

It is highly desirable to use simple and effective multiple access coding and decoding techniques which are capable of multiple access function and error control. The collaborative coding multiple access (CCMA) techniques potentially permit efficient simultaneous transmission by several users sharing a common channel, without subdivision in time, frequency or orthogonal **codes**. The **authors** investigate the performance of uniquely **decodable** CCMA schemes employing hard decision and maximum likelihood decoding techniques. A low complexity maximum likelihood decoding technique is presented. The reliability performance of various coding schemes employing these decoding techniques are carried out in the presence of AWGN conditions. The simulation results are presented in the form of symbol and codeword error rates as a function of signal to noise ratios. It is shown that uniquely decodable CCMA schemes permit the multiple access function to be combined with that of forward error correction.

23/5/5 (Item 5 from file: 8)

DIALOG(R)File 8: Ei Compendex(R)

(c) 2011 Elsevier Eng. Info. Inc. All rights reserved.

CROSS PARITY CHECK CONVOLUTION CODES FOR MAGNETIC TAPE.

Fuja, Tom; Heegard, Chris; Blaum, Mario

Corresp. Author/ Affil: Fuja, Tom: Cornell Univ, Ithaca, NY, USA, Cornell Univ, Ithaca, NY, USA

Conference Title: 1986 IEEE International Symposium on Information Theory (ISIT).

Conference Location: Ann Arbor, MI, USA

Sponsor: IEEE, Information Theory Group, New York, NY, USA

E.I. Conference No.: 9610

1986 , IEEE 86CH2374-7 (42-43)

Publication Date: 19861201

Publisher: IEEE

Document Type: Conference Paper; Conference Proceeding **Record Type:** Abstract

Language: English **Summary Language:** English

Summary form only given. The authors define and analyze cross parity check (CPC) convolutional codes, a class of error-control codes with both interesting theoretical properties and practical implementation advantages. CPC codes evolved from ideas used in an error-control scheme implemented on the IBM 3480 tape subsystem. The authors begin by placing both the 3840 code and its variation in a firm convolutional code context; specifically, they construct parity check matrices and describe systematic generators for these codes. They use the insight gained to define the class of CPC codes and to construct canonical parity check and generator matrices. They then prove that CPC codes are, in fact, maximum distance separable (MDS) convolution **codes**. The **authors** demonstrate how CPC encoding/ **decoding** delay can be shortened by 'folding' the parity check lines by dividing each term in the parity check matrix by some fixed polynomial, keeping only the remainder. In particular, they give a class of polynomials that, when used in this way, produce a code that is not only still MDS, but also retains much of its geometrical regularity.

23/5/8 (Item 1 from file: 2)
DIALOG(R)File 2: INSPEC
(c) 2011 The IET. All rights reserved.

A weakness in smart card PKI certification

Author(s): Young, A.
Book Title: IEEE Systems, Man and Cybernetics Society Information Assurance Workshop (IEEE Cat. No.03EX676)
Inclusive Page Numbers: 30-4
Publisher: IEEE, Piscataway, NJ
Country of Publication: USA
Publication Date: 2003
Conference Title: IEEE Systems, Man and Cybernetics Society Information Assurance Workshop
Conference Date: 18-20 June 2003
Conference Location: West Point, NY, USA
Number of Pages: 307
Language: English
Document Type: Conference Paper (PA)

Smartcards are becoming an integral part of public key infrastructures since they are separate computing devices that can store and utilize private keys without ever revealing them. Since the private keys are generated, stored, and used onboard to sign/decrypt data, smartcards are ideal when in the hands of a trusted private key owner. But, it is well known that nonreputability is only achieved when the private key owner does not expose his or her own private signing key. This implies that a very strong threat model exists in smartcard security: the user is not trusted to keep his or her own private key secret. It is a point in fact that corporations worldwide are concerned with this very problem and are making efforts to ensure that their employees cannot disclose their own signing private keys. An employee that could do so could later repudiate signatures on purchase orders, sales, and other legally binding transactions. A weakness in smart card PKI certification is shown that allows users to spoof the key generation processes on their smartcards and in effect grant them access to the bits of their private keys. A simple countermeasure is given that thwarts the possibility of this attack. (11 refs.)

23/5/13 (Item 6 from file: 2)
DIALOG(R)File 2: INSPEC
(c) 2011 The IET. All rights reserved.

VLSI array synthesis for polynomial GCD computation

Author(s): Jeong, Y.¹; Burleson, W.¹
Affiliation(s):
¹ Dept. of Electr. & Comput. Eng., Massachusetts Univ., Amherst, MA, USA
Book Title: Proceedings. International Conference on Application-Specific Array Processors (Cat. No.93TH0572-8)
Inclusive Page Numbers: 536-47
Publisher: IEEE Comput. Soc. Press, Los Alamitos, CA
Country of Publication: USA
Publication Date: 1993
Conference Title: Proceedings of International Conference on Application Specific Array Processors (ASAP'93)
Conference Date: 25-27 Oct. 1993
Conference Location: Venice, Italy
Conference Sponsor: Euromico
Editor(s): Dadda, L. Wah, B.
Item Identifier (DOI): [10.1109/ASAP.1993.397173](https://doi.org/10.1109/ASAP.1993.397173)
Number of Pages: xii+594
Language: English
Document Type: Conference Paper (PA)

Polynomial GCD (greatest common divisor) finding is an important problem in algebraic computation, especially in **decoding** error correcting **codes**. The **authors** show a new systolic array structure for the polynomial GCD problem using a systematic array synthesis technique. The VLSI implementation of the array structure is area-efficient and achieves maximum throughput with pipelining. The dependency graph (DG) of the Euclid GCD algorithm is drawn using iterated polynomial division. The resulting DG is data-dependent and variable-sized. The authors consider the worst-case implementation to make the DG data-dependent and fixed-size, where data-dependences are hidden inside by introducing four different working modes in each DG node. This novel approach requires just a few additional multiplexors and can be generalized for other data-dependent and variable-sized computation. The authors then map the DG to a one-dimensional systolic array using a linear mapping. The new array structure has $m_0 + n_0 + 1$ processing elements, where m_0 and n_0 are degrees of two polynomials. It can find a GCD of any two polynomials of total degree less than or equal to $m_0 + n_0$. The block pipeline period is one, which means that it can start a new GCD computation immediately in the next cycle. Unlike the array of Brent and Kung, a pre-processing step for extracting a common factor X^i is not necessary and the size of the processing element (PE) does not depend on m_0 and n_0 . The authors extend this new array structure to the extended polynomial GCD algorithm, which is closely related to the decoding of BCH and Reed-Solomon codes. To verify the structure, they have used the VERILOG simulator, and implemented a 2 μ CMOS test chip. (13 refs.)

23/5/15 (Item 8 from file: 2)

DIALOG(R)File 2: INSPEC

(c) 2011 The IET. All rights reserved.

Improved decoding algorithm on Reed-Solomon codes using division method

Author(s): Je Hong Jeong¹; Jin Soo Park

Affiliation(s):

¹ Dept. of Comput. Sci., Keonyang Univ., South Korea

Journal: Journal of the Korean Institute of Telematics and Electronics , vol.30A , no.11 , pp.21-8

Country of Publication: South Korea

Publication Date: Nov. 1993

Language: Korean

Document Type: Journal Paper (JP)

Decoding algorithm of noncyclic Reed-Solomon codes consists of four steps which are to compute syndromes, to find error-location polynomial, to decide error-location, and to solve error-values. There is a decoding method by which the computation of both error-location polynomial and error-polynomial can be avoided in conventional decoding methods using Euclid algorithm. The disadvantage of this method is that the same amount of computation is needed that is equivalent to solve the avoided polynomial. This paper considers the division method on polynomial on $GF(2^m)$ systematically. And proposes a novel method to find error correcting polynomial by simple mathematical expression without the same amount of computation to find the two avoided polynomials. Especially, the authors propose the method by which the amount of computation to find $F'(x)$ from the division $M(x)$ by x , $(x-1)$, \dots , $(x-\alpha^{n-2})$ respectively can be avoided. By applying the simple expression to **decoding** procedure on RS **codes**, the **authors** propose a new **decoding** algorithm, and to show the validity of present method, computer simulation is performed. (11 refs.)

23/5/23 (Item 16 from file: 2)

DIALOG(R)File 2: INSPEC

(c) 2011 The IET. All rights reserved.

Probability decoding of majority codes matched with APM signals

Author(s): Ankudinov, D.R.; Portnoy, S.L.

Journal: Elektrosvyaz , pp.13-17

Country of Publication: USSR

Translation Journal: Telecommunications and Radio Engineering, Part 1 (Telecommunications) , vol.44, no.8, pp.1-6

Publication Date of Translation Journal: Aug. 1989

Country of Publication of Translation Journal: USA

CODEN of Translation Journal: TCREAG

Language: English

Document Type: Journal Paper Translation Abstracted (JP)

The problem of increasing the efficiency of utilizing the frequency and power resources of information transmission systems is of great importance. One method for solving this problem is the matching of correcting codes with multiposition signals, achieved through the use of generalized cascade codes (GCC), whose internal codes form a system of embedded signal ensembles while the external codes are correcting **codes**. The **authors** discuss the coding and **decoding** of GCC and use the partial case of information transmission over a channel without memory, with additive white Gaussian noise of zero mean and variance, as an example. The method of 'soft' decoding of majority codes which have been matched with APM (amplitude-phase modulation) signals, and the method for calculating the empirical probabilities described, make it possible to synthesize GCC codecs with the described structure. Their use makes it possible to increase the power gain as a result of coding. (4 refs.)

23/5/25 (Item 18 from file: 2)

DIALOG(R)File 2: INSPEC

(c) 2011 The IET. All rights reserved.

Low cost security solutions for personal computers

Author(s): Schultz, J.B.

Journal: Signal , vol.44 , no.3 , pp.71-4

Country of Publication: USA

Publication Date: Nov. 1989

Language: English

Document Type: Journal Paper (JP)

Personal computer security advances in hardware and software systems are emerging in a host of new products in the commercial marketplace with applications to the Department of Defence and other government agencies. Designed for office and limited tactical applications, several of these off-the-shelf hardware and software devices commercially available cost less than \$300. Security features in some of these combination hardware/software or software only systems include the following: (i) automatic encryption/**decryption** of file directories; (ii) **owner** identification **codes** and passwords; (iii) secure transmission over modems; (iv) flexible security hierarchy. (5 refs.)

23/5/30 (Item 23 from file: 2)

DIALOG(R)File 2: INSPEC

(c) 2011 The IET. All rights reserved.

Video recorder programming with VPV

Journal: Funk-Technik , vol.41 , no.6 , pp.249-51

Country of Publication: West Germany

Publication Date: June 1986

Language: German

Document Type: Journal Paper (JP)

A simple procedure for the home programming of a novel video recorder using videotext to accept TV transmissions according to the VPS system, now widely employed by the two German networks (ARD, ZDF), is described in general terms. The recorder is the VPV model (acronym for videotext-programmed video-recorder), from the Thomson (old SABA) plant in Villengen. An additional bonus is the ability to display videotext pages via this recorder on any TV receiver, i.e. not having a videotext **decoder**. The **author** presents hexadecimal **code** words and equivalent screen symbols of the 7 controls and reproduce examples of a stored VPS program and selections from daily programs. (0 refs.)

23/5/32 (Item 25 from file: 2)

DIALOG(R)File 2: INSPEC

(c) 2011 The IET. All rights reserved.

An integrated approach to CD players. II. The decoding electronics

Author(s): Nijhof, J.

Journal: Electronic Components & Applications , vol.6 , no.4 , pp.216-22

Country of Publication: Netherlands

Publication Date: 1984

Language: English

Document Type: Journal Paper (JP)

For pt.I see *ibid.*, vol.6, no.4, p.209-15 (1984). Until now, no compact disc (CD) player has made full use of the error-correcting capability of the CD system's cross-interleaved Reed-Solomon **code** (CIRC). The **author** describes a **decoder** that can make the maximum four erasure corrections of this code. For errors that cannot be corrected by the CIRC, the decoder performs a basic interpolation. For full-performance players, a circuit that has an 8-sample interpolator and a new FIR digital filter with four times over sampling is available. In combination with a low-order analog filter, this digital filter produces no detectable sound coloration of the audio. (3 refs.)

23/5/36 (Item 29 from file: 2)

DIALOG(R)File 2: INSPEC

(c) 2011 The IET. All rights reserved.

Exponentiation modulo a polynomial for data security

Author(s): Kak, S.C.¹

Affiliation(s):

¹ Dept. of Electrical & Computer Engng., Louisiana State Univ., Baton Rouge, LA, USA

Journal: International Journal of Computer & Information Sciences , vol.12 , no.5 , pp.337-46

Country of Publication: USA

Publication Date: Oct. 1983

Language: English

Document Type: Journal Paper (JP)

This paper describes some properties of exponential modulo a polynomial and suggests its use for encryption in a mode that can be cryptanalysed in approximately $O(pd^3)$ time, where d is the size of the message frame and p is the prime modulo which the rankwise computations are carried out. While for sufficiently large $pd(\sim 10^5)$ this appears to provide a one-way function which can be used in a public-key cryptosystem, the **author** shows that since encryption/**decryption** effort is defined in $O(d^2 \log pd \log \log p)$ time, a practical application of the proposed algorithm would be either in a secret key or in a tamper-proof, hardwired secret polynomial system. (8 refs.)

23/5/56 (Item 2 from file: 99)

DIALOG(R)File 99: Wilson Appl. Sci & Tech Abs

(c) 2011 The HW Wilson Co. All rights reserved.

A modified learning rule of the neural network for error correcting decoding

Augmented Title: discussion of A neural network for error correcting decoding of binary linear codes by Anna Esposito, Salvatore Rampone and Roberto Tagliaferri

Lifang Li ; Zhigang Cao

Neural Networks v. 10 (Mar. '97) p. 387-8

Document Type: Feature Article **ISSN:** 0893-6080 **Language:** English **Record Status:** Corrected or revised record

In a discussion of the 1994 article by Esposito et al. describing a neural network for error correcting **decoding** of binary linear **codes**, the **writers** propose a modified learning rule for the neural network described. Using the new training and tuning method, it is proved that the network can be extended for all binary linear codes and complementary codes regardless of their maximum Hamming weights.

23/5/63 (Item 2 from file: 60)

DIALOG(R)File 60: ANTE: Abstracts in New Tech & Engineer

(c) 2011 CSA. All rights reserved.

Method and apparatus for enhancing software security and distributing software

Chang, Sheue-Ling; Gosling, James , USA

Publisher Url: <http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=/netahtml/PTO/search-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=5724425.PN.&OS=pn/5724425&RS=PN/5724425>

Document Type: Patent **Record Type:** Abstract

Language: English

Source code to be protected, a software application writer's private key, along with an application writer's license provided to the first computer. The application writer's license includes identifying information such as the application writer's name as well as the application writer's public key. A compiler program executed by the first computer compiles the source code into binary code, and computes a message digest for the binary code. The first computer then encrypts the message digest using the application writer's private key, such that the encrypted message digest is defined as a digital 'signature' of the application writer. A software passport is then generated which includes the application writer's digital signature, the application writer's license and the binary code. The software passport is then distributed to a user using any number of software distribution models known in the industry. A user, upon receipt of the software passport, loads the passport into a computer which determines whether the software passport includes the application writer's license and digital signature. In the event that the software passport does not include the application writer's license, or the application writer's digital signature, then the user's computer system discards the software passport and does not execute the binary code. As an additional security step, the user's computer computes a second message digest for the software passport and compares it to the first message digest, such that if the first and second message digests are not equal, the software passport is also rejected by the user's computer and the code is not executed. If the first and second message digests are equal, the user's computer extracts the application writer's public key from the application writer's license for verification. The application **writer's** digital **signature** is **decrypted** using the application **writer's** public **key**. The user's computer then compares a message digest of the binary code to be executed, with the **decrypted** application **writer's** digital **signature**, such that if they are equal, the user's computer executes the binary code.

23/5/64 (Item 3 from file: 60)

DIALOG(R)File 60: ANTE: Abstracts in New Tech & Engineer

(c) 2011 CSA. All rights reserved.

Authoring system, authoring key generator, authoring device, authoring method, and data supply device, information terminal and information distribution method

Yamanaka, Yasuhiro; Yoshitomi, Kazunori; Hisamatsu, Fumiaki; Yoshino, Kenji ; Ueno, Shinichi , USA

Publisher Url: <http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=/netahtml/PTO/search-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=7328458.PN.&OS=pn/7328458&RS=PN/7328458>

Document Type: Patent **Record Type:** Abstract

Language: English

An authoring system authors content data for distribution through an information terminal by encryption for copyright protection. The system includes an authoring device and an authoring key generator. The generator generates a content identifier uniquely allocated to each of the content data, an authoring key enabling key uniquely allocated to the authoring device, and an authoring key obtained by encrypting a content key for encrypting the content data and a second content key using the CID and the CEK. The second content key is formed by encrypting the content key using a root **key**. The **authoring** device has a unit which **decrypts** the content key and the second content key using the CID and the CEK, and a unit which encrypts the content data using the decrypted content key to generate authored encrypted content data.

28/5/1 (Item 1 from file: 8)
DIALOG(R)File 8: Ei Compendex(R)
(c) 2011 Elsevier Eng. Info. Inc. All rights reserved.

Approaches to biometric watermarks for owner authentication

Vielhauer, C.; Steinmetz, R.

Corresp. Author/ Affil: Vielhauer, C.: 1-Platanista GmbH, Darmstadt, 64289, Germany

Editor(s): Wong, P.W.; Delp, E.J.

Editor(s) Affil.: Apalo.com Ltd., Hong Kong, China

Conference Title: Security and Watermarking of Multimedia Contents III

Conference Location: San Jose, CA United States **Conference Date:** 20010122-20010125

Sponsor: IS and T; SPIE

E.I. Conference No.: 58754 **Proceedings of SPIE - The International Society for Optical Engineering**
(Proc SPIE Int Soc Opt Eng) (United States) 2001 4314/- (209-219)

Publication Date: 20011113

Publisher: SPIE

Item Identifier (DOI): [10.1117/12.435401](https://doi.org/10.1117/12.435401)

Document Type: Conference Paper; Conference Proceeding **Record Type:** Abstract

Language: English **Summary Language:** English

Number of References: 15

One major application domain for digital watermarks is **copyright protection**. Besides the design of watermarking algorithms, technologies for copyright holder identification have to be investigated. To ensure authenticity of an individual person, a wide number of biometric procedures exist. We define and describe new biometric watermarks, which denote the application of biometric reference data of individuals within digital watermarks to identify and verify ownership. Amongst the two classes of physiological and senso-motoric biometric schemes, the later appears more appropriate for biometric watermarks, as only these provide implicit expressions of intention. As such, we choose on-line handwriting as an appropriate base technology for our three new scenarios in biometric watermarking. In the first approach, embedding keys are being generated from biometric reference data, which requires stable and robust features and leads to rather complex keys. To overcome the complexity boundaries, the second approach develops a biometric reference hash, allowing key look-ups in key certifying servers. Although this proceeding leads to less complex keys, it still requires stable features. The third approach describes the embedding of biometric reference data within a watermark, allowing owner verification by more variant features, but limitations apply due to capacity of watermarking systems and also protection of the reference data is required. While most handwriting-based verification systems are limited to signature contexts, we discuss two additional context types for user authentication: passphrases and sketches.

28/5/2 (Item 1 from file: 2)
DIALOG(R)File 2: INSPEC
(c) 2011 The IET. All rights reserved.

An introduction to servo pneumatic positioning: an interactive multimedia program development supporting outcome-driven engineering assessment

Author(s): Ranky, P.G.; Ranky, M.F.; Flaherty, M.; Sands, S.; Stratful, S.

Journal: European Journal of Engineering Education , vol.23 , no.3 , pp.339-52

Publisher: Carfax

Country of Publication: UK

Publication Date: Sept. 1998

Language: English

Document Type: Journal Paper (JP)

Servo pneumatics retain the advantages of standard pneumatics and add the opportunity for closed-loop controlled, programmable positioning to within fractions of a millimeter in systems in which positions can be approached rapidly and without overshoot, stability under variable loads and conditions, and adaptive control for optimized positioning. The authors' challenge was to create an interactive multimedia program that could communicate exciting technical material to interested

parties, including students and academia, professional design, industrial and manufacturing systems engineers, marketing and sales engineers and managers in a nonlinear, enjoyable fashion. Their approach was that of interactive multimedia on **CD-ROM**, allowing the integration of text, color images, videos and animation for the purpose of following an engineering problem-solving approach, both when modeling, as well as when illustrating real-world solutions with interactive digital videos. Furthermore, this article introduces outcome-driven assessment principles (as defined by the American Accreditation Board of Engineering Education) as the **key** to the **authors'** educational multimedia design objectives. It illustrates open-loop controlled pneumatic and closed-loop controlled servo pneumatic positioning systems, their components, their programming and some of their applications. (21 refs.)

28/5/3 (Item 2 from file: 2)
DIALOG(R)File 2: INSPEC
(c) 2011 The IET. All rights reserved.

Today's best CD-ROM books

Author(s): Reese, J.¹

Affiliation(s):

¹ Educ. Libr., Vanderbilt Univ., Nashville, TN, USA

Journal: CD-ROM Professional , vol.7 , no.1 , pp.119-21

Country of Publication: USA

Publication Date: Jan. 1994

Language: English

Document Type: Journal Paper (JP)

The literature of **CD-ROM** has exploded in the last several years. As **CD-ROM** technology demonstrates its staying power and continued growth, publishers have turned out more sources for interested users. The **author** provides some **key** books, both directories and other resources, to keep in mind whether you need to purchase **CD-ROM** products or just learn more about what's going on in the world of **CD-ROM**. (0 refs.)

28/5/4 (Item 3 from file: 2)
DIALOG(R)File 2: INSPEC
(c) 2011 The IET. All rights reserved.

Performance of modulation codes in various optical recording media

Author(s): van Uijen, C.M.J.¹; Spruit, J.H.M.¹

Affiliation(s):

¹ Philips Res. Labs., Eindhoven, Netherlands

Journal: Japanese Journal of Applied Physics, Part 1 (Regular Papers & Short Notes) , vol.31 , no.2B , pp.670-9

Country of Publication: Japan

Publication Date: Feb. 1992

Language: English

Document Type: Journal Paper (JP)

The performance of modulation codes has been measured in ablative and magneto-optic **recording media** as well as in mastered direct discs. The modulation codes studied include NRZ (i.e. the uncoded bit stream), runlength limited sequences, multi-level recording schemes, and differentially detectable **codes**. The **authors** also studied the performance of codes when the optical channel is equalised, particularly the case of partial response detection of NRZ. The general conclusions are that: (1) differentially detectable codes require the full penalty in data density caused by the loss in code rate, (2) multi-level recording does not offer significant advantages, and step-constrained multi-level codes perform worse than their unconstrained counterparts, (3) runlength limited sequences are useful codes to enhance the density while offering additional practical advantages, and (4) partial response detection of uncoded bit streams transmitted through an equalised optical recording channel achieves the highest density. (12 refs.)

28/5/5 (Item 4 from file: 2)
DIALOG(R)File 2: INSPEC
(c) 2011 The IET. All rights reserved.

A watermarking technique robust to spatial scaling for moving picture application

Author(s): Min-Suk Hong¹; Tae-Yun Chung¹; Kang-Seo park; Sang-Hui Park

Affiliation(s):

¹ Dept. of Electr. & Comput. Eng., Yonsei Univ., Seoul, South Korea

Journal: Journal of Electrical Engineering and Information Science , vol.5 , no.3 , pp.209-17

Publisher: Korean Inst. Electr. Eng.

Country of Publication: Taiwan

Publication Date: June 2000

Language: English

Document Type: Journal Paper (JP)

The digital watermarking has been proposed to protect copyright by embedding an invisible signal. We present a private/public key watermarking technique robust to spatial scaling. The private key is used to identify the copyright owner of digital video data, while the public key is used to embed copy control data. The proposed algorithm uses a synchronization code to accomplish the robustness to spatial scaling such as aspect ratio conversion and resampling for a spatial scalability hierarchy. We performed MPEG2 video compression for test sequences to evaluate the degradation of image quality caused by watermark insertion. In order to evaluate the geometrical robustness, we have performed 16:9 or 4:3 aspect ratio conversion for test sequences. We obtained watermarked frames that have no perceptual difference from the original frame and the geometrically robust watermark algorithm. (10 refs.)

28/5/6 (Item 1 from file: 60)
DIALOG(R)File 60: ANTE: Abstracts in New Tech & Engineer
(c) 2011 CSA. All rights reserved.

Authoring system, authoring key generator, authoring device, authoring method, and data supply device, information terminal and information distribution method

Yamanaka, Yasuhiro; Yoshitomi, Kazunori; Hisamatsu, Fumiaki; Yoshino, Kenji ; Ueno, Shinichi , USA

Publisher Url: <http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=/netahtml/PTO/search-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=7328458.PN.&OS=PN/7328458&RS=PN/7328458>

Document Type: Patent **Record Type:** Abstract

Language: English

An authoring system authors content data for distribution through an information terminal by encryption for **copyright protection**. The system includes an authoring device and an **authoring key generator**. The generator generates a content identifier uniquely allocated to each of the content data, an **authoring key enabling key** uniquely allocated to the authoring device, and an **authoring key** obtained by encrypting a content key for encrypting the content data and a second content key using the CID and the CEK. The second content key is formed by encrypting the content key using a root **key**. The **authoring device** has a unit which decrypts the content key and the second content key using the CID and the CEK, and a unit which encrypts the content data using the decrypted content key to generate authored encrypted content data.